PGP® Desktop für Windows

Benutzerhandbuch

Versionsinformationen

PGP Desktop für Windows Benutzerhandbuch. PGP Desktop Version 10.0.3. Veröffentlichungsdatum: Oktober 2010.

Copyright-Informationen

Copyright © 1991-2010, PGP Corporation. Alle Rechte vorbehalten. Dieses Dokument darf ohne ausdrückliche schriftliche Genehmigung der PGP Corporation weder im Ganzen noch in Teilen, in keiner Form und auf keine Weise, weder mechanisch noch elektronisch und zu keinem Zweck vervielfältigt oder weitergegeben werden.

Markeninformationen

PGP, Pretty Good Privacy und das PGP-Logo sind in den USA und anderen Ländern eingetragene Marken der PGP Corporation. IDEA ist eine Marke der Ascom Tech AG. Windows und ActiveX sind eingetragene Marken der Microsoft Corporation. AOL ist eine eingetragene Marke und AOL Instant Messenger ist eine Marke von America Online, Inc. Red Hat und Red Hat Linux sind Marken oder eingetragene Marken von Red Hat, Inc. Linux ist eine eingetragene Marke von Linus Torvalds. Solaris ist eine Marke oder eingetragene Marke von Sun Microsystems, Inc. AIX ist eine Marke oder eingetragene Marke von International Business Machines Corporation. HP-UX ist eine Marke oder eingetragene Marke der Hewlett-Packard Company. SSH und Secure Shell sind Marken von SSH Communications Security, Inc. Rendezvous und Mac OS X sind Marken oder eingetragene Marken von Apple Computer, Inc. Alle anderen eingetragenen und nicht eingetragenen Marken, die in diesem Dokument erwähnt werden, sind alleiniges Eigentum ihrer jeweiligen Inhaber.

Lizenzierungs- und Patentinformationen

Der IDEA-Kryptografiealgorithmus, der in US-Patent Nr. 5.214.703 beschrieben wird, wurde von der Ascom Tech AG lizenziert. Der Verschlüsselungsalgorithmus CAST-128, der im RFC 2144 beschrieben wird, ist weltweit für kommerzielle und nicht kommerzielle Zwecke ohne Lizenzgebühren freigegeben. Die PGP Corporation hat sich eine Lizenz auf die Patentrechte im Patentantrag des Aufsichtskomitees der University of California mit der Seriennummer 10/655.563 und dem Titel „Block Cipher Mode of Operation for Constructing a Wide-blocksize block Cipher from a Conventional Block Cipher“ gesichert. Teile der Software von Drittanbietern, die in PGP Universal Server enthalten sind, sind gemäß der GNU General Public License (GPL) lizenziert. PGP Universal Server als Ganzes ist nicht gemäß der GPL lizenziert. Wenn Sie eine Kopie des Quellcodes der in PGP Universal Server enthaltenen GPL-Software anfordern möchten, wenden Sie sich an den *PGP-Support* (https://support.pgp.com). Die PGP Corporation verfügt möglicherweise über Patente und/oder zum Patent angemeldete Anwendungen für Inhalte dieser Software oder ihrer Dokumentation. Mit der Bereitstellung dieser Software oder Dokumentation werden Ihnen keine Lizenzrechte für besagte Patente übertragen.

Danksagungen

Dieses Produkt kann Folgendes enthalten:

● Die von Mark Adler und Jean-Loup Gailly erstellten Komprimierungscodes Zip und ZLib werden mit Genehmigung der kostenlosen Info-ZIP-Implementierung verwendet, die von zlib (http://www.zlib.net) entwickelt wurde. ● Libxml2, der XML C-Parser und das XML C-Toolkit, die für das Gnome-Projekt entwickelt wurden und gemäß der MIT-Lizenz (http://www.opensource.org/licenses/mit-license.html) vertrieben werden und urheberrechtlich geschützt sind. Copyright © 2007, Open Source Initiative. ● bzip2 1.0, eine kostenlos verfügbare hochwertige Datenkomprimierungsanwendung, urheberrechtlich geschützt durch Julian Seward, © 1996-2005. ● Anwendungsserver (http://jakarta.apache.org/), Webserver (http://www.apache.org/), Jakarta Commons (http://jakarta.apache.org/commons/license.html) und log4j, eine auf Java basierende Bibliothek für die Analyse von HTML, entwickelt von der Apache Software Foundation. Die Lizenz ist unter www.apache.org/licenses/LICENSE-2.0.txt verfügbar. ● Castor, ein auf Open Source basierendes Datenbindungs-Framework zum Übertragen von Daten aus XML in Java-Objekte und aus Java in Datenbanken, wird von der ExoLab Group gemäß einer Apache 2.0-ähnlichen Lizenz veröffentlicht, die unter http://www.castor.org/license.html verfügbar ist. ● Xalan, eine Open-Source-Softwarebibliothek der Apache Software Foundation, die die XML-Transformationssprache XSLT und die XML-Abfragesprache XPath implementiert, wird gemäß der Apache Software-Lizenz Version 1.1 veröffentlicht, die unter http://xml.apache.org/xalan-j/#license1.1 verfügbar ist. ● Apache Axis, eine Implementierung von SOAP (Simple Object Access Protocol), die für Kommunikationen zwischen verschiedenen PGP-Produkten verwendet wird, wird gemäß der Apache-Lizenz bereitgestellt, die unter http://www.apache.org/licenses/LICENSE-2.0.txt verfügbar ist. ● mx4j, eine Open-Source-Implementierung der Java Management Extensions (JMX), wird gemäß einer Apache-ähnlichen Lizenz veröffentlicht, die unter http://mx4j.sourceforge.net/docs/ch01s06.html verfügbar ist. ● jpeglib Version 6a basiert teilweise auf den Arbeiten der Independent JPEG Group (http://www.ijg.org/). ● libxslt, eine XSLT C-Bibliothek, die für das GNOME-Projekt entwickelt wurde und für XML-Transformationen verwendet wird, wird gemäß der MIT-Lizenz (http://www.opensource.org/licenses/mit-license.html) vertrieben. ● Perl-Compiler für reguläre Ausdrücke, PCRE Version 4.5, urheberrechtlich geschützt und vertrieben von der University of Cambridge. ©1997-2006. Das Lizenzabkommen ist unter http://www.pcre.org/license.txt verfügbar. ● BIND-Protokolle für Balanced Binary Tree Library und Domain Name System (DNS), von Internet Systems Consortium, Inc. (http://www.isc.org) entwickelt und urheberrechtlich geschützt. ● Kostenlose BSD-Implementierung von Daemon, entwickelt von The FreeBSD Project, © 1994-2006. ● Simple Network Management Protocol Library, entwickelt und urheberrechtlich geschützt von der Carnegie Mellon University, © 1989, 1991, 1992, Networks Associates Technology, Inc, © 2001-2003, Cambridge Broadband Ltd., © 2001-2003, Sun Microsystems, Inc., © 2003, Sparta, Inc, © 2003-2006, Cisco, Inc. und Information Network Center of Beijing University of Posts and Telecommunications, © 2004. Das Lizenzabkommen hierfür ist unter http://net-snmp.sourceforge.net/about/license.html verfügbar. ● NTP Version 4.2, entwickelt von Network Time Protocol und von mehreren Beitragenden urheberrechtlich geschützt ● Lightweight Directory Access Protocol, entwickelt und urheberrechtlich geschützt von der OpenLDAP Foundation. OpenLDAP ist eine Open-Source-Implementierung des Lightweight Directory Access Protocol (LDAP). Copyright © 1999-2003, The OpenLDAP Foundation. Das Lizenzabkommen ist unter http://www.openldap.org/software/release/license.html verfügbar. Secure Shell OpenSSH, Version 4.2.1, entwickelt und veröffentlicht vom OpenBSD Project gemäß einer BSD-ähnlichen Lizenz, die unter http://www.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/LICENCE?rev=HEAD verfügbar ist. ● PC/SC Lite ist eine kostenlose Implementierung von PC/SC, einer Spezifikation für die Integration von Smartcards, die gemäß der BSD-Lizenz veröffentlicht wird. ● Postfix, ein Mail Transfer Agent (MTA) auf Open-Source-Basis, wird gemäß der IBM Public License 1.0 veröffentlicht, die unter http://www.opensource.org/licenses/ibmpl.php verfügbar ist. ● PostgreSQL, ein kostenloses objektrelationales Datenbankverwaltungssystem, wird gemäß einer BSD-ähnlichen Lizenz veröffentlicht, die unter http://www.postgresql.org/about/licence verfügbar ist. ● PostgreSQL-JDBC-Treiber, ein kostenloses Java-Programm zum Herstellen einer Verbindung mit PostgreSQL-Datenbanken über standardmäßigen, datenbankunabhängigen Java-Code, (c) 1997-2005, PostgreSQL Global Development Group, wird gemäß einer BSD-ähnlichen Lizenz veröffentlicht, die unter http://jdbc.postgresql.org/license.html verfügbar ist. ● PostgreSQL Regular Expression Library, ein kostenloses objektrelationales Datenbankverwaltungssystem, wird gemäß einer BSD-ähnlichen Lizenz veröffentlicht, die unter http://www.postgresql.org/about/licence verfügbar ist. ● 21.vixie-cron ist die Vixie-Version von cron, einem UNIX-Standarddaemon, der bestimmte Programme zu vorgegebenen Zeiten ausführt. Copyright © 1993, 1994, Paul Vixie; mit Genehmigung verwendet. ● JacORB, ein Java-Objekt, das zur Verbesserung der Kommunikation zwischen in Java geschriebenen Prozessen und der Datenschicht verwendet wird, wird als Open Source gemäß der GNU Library General Public License (LGPL) lizenziert, die unter http://www.jacorb.org/lgpl.html verfügbar ist. Copyright © 2006 The JacORB Project. ● TAO (The ACE ORB) ist eine Open-Source-

Implementierung eines CORBA Object Request Broker (ORB) und wird zur Kommunikation zwischen in C/C++ geschriebenen Prozessen und der Datenschicht verwendet. Copyright (c) 1993-2006, Douglas C. Schmidt und seine Forschungsgruppe an der Washington University, der University of California, Irvine und der Vanderbilt University. Die Open-Source-Softwarelizenz ist unter http://www.cs.wustl.edu/~schmidt/ACE-copying.html verfügbar. ● libcURL, eine Bibliothek zum Herunterladen von Dateien über gemeinsame Netzwerkdienste, ist eine Open-Source-Software, die gemäß einer Ableitung der MIT/X-Lizenz bereitgestellt wird, die unter http://curl.haxx.se/docs/copyright.html verfügbar ist. Copyright (c) 1996-2007, Daniel Stenberg. ● libuuid, eine Bibliothek zur Erstellung eindeutiger Bezeichner, wird gemäß einer BSD-ähnlichen Lizenz veröffentlicht, die unter http://thunk.org/hg/e2fsprogs/?file/fe55db3e508c/lib/uuid/COPYING verfügbar ist. Copyright (C) 1996, 1997 Theodore Ts'o. ● libpopt, eine Bibliothek zum Analysieren von Befehlszeilenoptionen, wird gemäß den Bestimmungen der GNU Free Documentation License veröffentlicht, die unter http://directory.fsf.org/libs/COPYING.DOC verfügbar ist. Copyright © 2000-2003 Free Software Foundation, Inc. ● gSOAP, ein Entwicklungstool für Windows-Clients für die Kommunikation mit dem AMT-Chipsatz der Intel Corporation auf der Hauptplatine, wird gemäß der GNU Public License bereitgestellt, die unter http://www.cs.fsu.edu/~engelen/soaplicense.html verfügbar ist. ● Die Windows Template Library (WTL) wird zur Entwicklung von Komponenten der Benutzeroberfläche verwendet und gemäß der Common Public License v1.0 bereitgestellt, die unter http://opensource.org/licenses/cpl1.0.php verfügbar ist. ● Das Perl-Kit umfasst mehrere unabhängige Dienstprogramme für die Automatisierung verschiedener Verwaltungsfunktionen und wird gemäß der Perl Artistic License bereitgestellt, die unter http://www.perl.com/pub/a/language/misc/Artistic.html verfügbar ist. ● rEFIt - libeg stellt eine graphische Schnittstellenbibliothek für EFI bereit, einschließlich Bild- und Textwiedergabe sowie Alpha-Blending, und wird gemäß der Lizenz bereitgestellt, die unter http://refit.svn.sourceforge.net/viewvc/*checkout*/refit/trunk/refit/LICENSE.txt?revision=288 verfügbar ist. Copyright (c) 2006 Christoph Pfisterer. Alle Rechte vorbehalten. ● Java Radius Client für die Authentifizierung von PGP Universal Web Messenger-Benutzern über Radius, wird gemäß der Lesser General Public License (LGPL) bereitgestellt, die unter http://www.gnu.org/licenses/lgpl.html verfügbar ist. ● Yahoo! User Interface (YUI)-Bibliothek, Version 2.5.2, eine Webbenutzeroberflächen-Schnittstellenbibliothek für AJAX. Copyright (c) 2009, Yahoo! Inc. Alle Rechte vorbehalten. Veröffentlicht gemäß einer BSD-ähnlichen Lizenz, die unter http://developer.yahoo.com/yui/license.html verfügbar ist. ● JSON-lib, Version 2.2.1, eine Java-Bibliothek, die zum Konvertieren von Java-Objekten in JSON-Objekte (JavaScript Object Notation) für AJAX verwendet wird. Bereitgestellt gemäß der Apache 2.0-Lizenz, die unter http://json-lib.sourceforge.net/license.html verfügbar ist. ● EZMorph, verwendet von JSON-lib, wird gemäß der Apache 2.0-Lizenz bereitgestellt, die unter http://ezmorph.sourceforge.net/license.html verfügbar ist. ● Apache Commons Lang, verwendet von JSON-lib, wird gemäß der Apache 2.0-Lizenz bereitgestellt, die unter http://commons.apache.org/license.html verfügbar ist. ● Apache Commons BeanUtils, verwendet von JSON-lib, wird gemäß der Apache 2.0-Lizenz bereitgestellt, die unter http://commons.apache.org/license.html verfügbar ist.

Exportinformationen

Der Export dieser Software und ihrer Dokumentation unterliegt u. U. den entsprechenden Durchführungsbestimmungen des Bureau of Export Administration, United States Department of Commerce, die den Export und Reexport von bestimmten Produkten und technischen Daten einschränken.

Nutzungseinschränkungen

Die Software, zu der diese Dokumentation gehört, wird Ihnen für die persönliche Nutzung zu den Bedingungen lizenziert, die im mit der Software gelieferten Endbenutzerlizenzabkommen (EULA) aufgeführt sind. Die Informationen in diesem Dokument können ohne Vorankündigung geändert werden. Die PGP Corporation garantiert nicht, dass die Informationen Ihre Anforderungen erfüllen oder dass sie fehlerfrei sind. Die Informationen können technische Ungenauigkeiten oder Tippfehler enthalten. Diese Informationen können geändert werden und in neuen Ausgaben dieses Dokuments enthalten sein, falls diese ggf. von der PGP Corporation zur Verfügung gestellt werden.

Inhalt

Informationen zu PGP Desktop 10.0 für Windows 1

Neuheiten bei PGP Desktop für Windows Version 10.0 2
Neuerungen in PGP Desktop 10.0 2
Dieses Handbuch verwenden 5
„Zentral verwaltete“ und „Einzelplatz“-Benutzer 5
In diesem Handbuch verwendete Konventionen 6
Adressaten dieses Dokuments 7
Informationen zur Lizenzierung von PGP Desktop 7
PGP Desktop für Windows lizenzieren 7
Lizenzdetails prüfen 8
Ablauf der Lizenz 10
Hilfe und Support 11
Informationen zum Produkt 11
Kontaktinformationen 12

PGP Desktop-Grundlagen 13

PGP Desktop-Grundbegriffe 13
PGP-Produktkomponenten 13
In PGP Desktop verwendete Begriffe 15
Konventionelle Kryptografie und Kryptografie mit öffentlichen Schlüsseln 17
Mehr über Kryptographie erfahren 18
PGP Desktop erstmals verwenden 18

PGP Desktop installieren 21

Installation vorbereiten 21
Systemvoraussetzungen 21
Kompatibilität mit Citrix und Terminal-Services 22
PGP Desktop installieren und konfigurieren 22
Software installieren 23
Software-Upgrade 23
Lizenzierung von PGP Desktop 26
Einrichtungsassistenten ausführen 26
Option zum Deinstallieren von PGP Desktop 26
PGP Desktop-Installation von einem Computer auf einen anderen übertragen 27

Benutzeroberfläche von PGP Desktop 29

Auf PGP Desktop-Funktionen zugreifen 29
Hauptbildschirm von PGP Desktop 30
PGP-Symbol im Infobereich der Taskleiste verwenden 31
Kontextmenüs in Windows Explorer verwenden 34

Startmenü verwenden 35
Notifier-Warnungen von PGP Desktop 36
PGP Desktop Notifier für Messaging 36
PGP Desktop Notifier für Laufwerksfunktionen 39
Notifier-Meldungen aktivieren oder deaktivieren 40
PGP-Protokoll anzeigen 41

Mit PGP Keys arbeiten 43

Schlüssel anzeigen 43
Schlüsselpaare erstellen 44
Kennwörter und Passphrasen 47
Privaten Schlüssel schützen 48
Schlüssel und Schlüsselbunde schützen 49
Sicherungskopien von privaten Schlüsseln erstellen 50
Vorgehensweise bei verlorenen Schlüsseln 50
Öffentliche Schlüssel verteilen 51
Öffentliche Schlüssel auf einem Keyserver ablegen 51
Öffentliche Schlüssel in E-Mail-Nachrichten einfügen 53
Öffentliche Schlüssel in Dateien exportieren 53
Direkt von einer Smartcard auf den Schlüsselbund einer anderen Person kopieren 54
Öffentliche Schlüssel anderer Personen erhalten 54
Öffentliche Schlüssel von einem Keyserver abrufen 55
Öffentliche Schlüssel aus E-Mail-Nachrichten übernehmen 56
Mit Keyservern arbeiten 56
Hauptschlüssel verwenden 58
Der Hauptschlüsselliste Schlüssel hinzufügen 58
Schlüssel aus der Hauptschlüsselliste löschen 59

PGP-Schlüssel verwalten 61

Schlüsseleigenschaften anzeigen und festlegen 62
Mit Foto-IDs arbeiten 63
Benutzernamen und E-Mail-Adressen in einem Schlüssel verwalten 64
Schlüssel und X.509-Zertifikate importieren 65
Den Assistenten für den Zertifikatimport verwenden 66
Passphrase ändern 68
Schlüssel, Benutzer-IDs und Signaturen löschen 69
Öffentliche Schlüssel deaktivieren und aktivieren 70
Einen öffentlichen Schlüssel verifizieren 71
Öffentliche Schlüssel signieren 72
Signaturen von öffentlichen Schlüsseln widerrufen 74
Vertrauen für Schlüsselvalidierungen gewähren 74
Mit Unterschlüsseln arbeiten 75
Separate Unterschlüssel verwenden 77
Unterschlüssel anzeigen 78
Neue Unterschlüssel erstellen 78
Schlüsselverwendung für Unterschlüssel festlegen 79

Unterschlüssel widerrufen 81
Unterschlüssel entfernen 81
Mit ADKs arbeiten 81
ADKs zu einem Schlüsselpaar hinzufügen 82
Einen ADK aktualisieren 83
ADKs entfernen 83
Mit Widerrufern arbeiten 83
Designierte Widerrufer zu Schlüsseln hinzufügen 84
Schlüssel widerrufen 84
Schlüssel teilen und wieder zusammenfügen 85
Geteilte Schlüssel erstellen 85
Geteilte Schlüssel wieder zusammenfügen 87
Vorgehensweise bei verloren gegangenen Schlüsseln oder Passphrasen 89
Schlüssel mit PGP Universal Server wiederherstellen 89
Schlüsselwiederherstellungsdaten erstellen 90
Schlüssel bei verloren gegangenen Schlüsseln bzw. Passphrasen wiederherstellen 92
Schlüssel schützen 94

E-Mail-Nachrichten sichern 95

E-Mail-Nachrichten mit PGP Desktop sichern 95
Eingehende Nachrichten 97
Ausgehende Nachrichten 98
MAPI-E-Mail-Nachrichten mit Microsoft Outlook senden 99
Signier- und Verschlüsselungsschaltflächen in Microsoft Outlook verwenden 100
Offline-Richtlinien verwenden 101
Dienste und Richtlinien 103
Dienste und Richtlinien anzeigen 104
Neue Messaging-Dienste erstellen 106
Eigenschaften des Messaging-Dienstes bearbeiten 110
Dienste deaktivieren oder aktivieren 110
Dienste löschen 111
Mehrere Dienste 111
Problembehebung bei PGP Messaging-Diensten 112
Neue Sicherheitsrichtlinien erstellen 114
Reguläre Ausdrücke in Richtlinien 120
Informationen und Beispiele zu Sicherheitsrichtlinien 122
Mit der Sicherheitsrichtlinienliste arbeiten 127
Sicherheitsrichtlinien bearbeiten 127
Adressenlisten-Richtlinien bearbeiten 128
Sicherheitsrichtlinien löschen 133
Reihenfolge der Richtlinien in der Liste ändern 134
PGP Desktop und SSL 134
Schlüsselmodi 136
Schlüsselmodus ermitteln 138
Schlüsselmodus ändern 138

PGP-Protokoll anzeigen 140

Instant Messaging-Sitzungen sichern 143

Informationen zur Instant Messaging-Kompatibilität von PGP Desktop 143
Kompatibilität mit Instant Messaging-Clients 144
Informationen zu den für die Verschlüsselung verwendeten Schlüsseln 145
IM-Sitzungen verschlüsseln 145

E-Mail-Nachrichten mit PGP Viewer anzeigen 147

Übersicht über PGP Viewer 147
Kompatible E-Mail-Clients 148
Verschlüsselte E-Mail-Nachrichten oder Dateien öffnen 149
E-Mail-Nachrichten in den Posteingang kopieren 150
E-Mail-Nachrichten exportieren 151
Zusätzliche Optionen angeben 151
Optionen in PGP Viewer festlegen 151
Sicherheitsfunktionen in PGP Viewer 152

Laufwerke mit PGP Whole Disk Encryption schützen 155

Informationen zu PGP Whole Disk Encryption 156
Worin unterscheidet sich PGP Whole Disk Encryption von PGP Virtual Disk? 158
PGP Whole Disk Encryption lizenzieren 158
Ablauf der Lizenz 159
Laufwerk auf die Verschlüsselung vorbereiten 159
Unterstützte Laufwerkstypen 160
Unterstützte Tastaturen 161
Laufwerksintegrität vor der Verschlüsselung sicherstellen 164
Verschlüsselungsdauer berechnen 164
Netzbetrieb während der Verschlüsselung beibehalten 165
Pilotversuch zum Sicherstellen der Softwarekompatibilität durchführen 166
Authentifizierungsmethode für das Laufwerk bestimmen 167
Passphrasen- und Einzelanmeldungsauthentifizierung 167
Authentifizierung mit öffentlichen Schlüsseln 168
Token-basierte Authentifizierung 168
Zweistufige Authentifizierung mit einem USB-Flash-Gerät 168
Authentifizierung über das Trusted Platform Module (TPL) 169
Verschlüsselungsoptionen festlegen 170
Verschlüsselung auf Partitionsebene 171
Smartcard oder Token zur Verwendung für die Authentifizierung vorbereiten 172
Optionen von PGP Whole Disk Encryption verwenden 175
Laufwerke oder Partitionen verschlüsseln 177
Unterstütze Zeichen für Passphrasen für PGP Whole Disk Encryption 178
Laufwerk verschlüsseln 179
Laufwerksfehler während der Verschlüsselung 183

Mit PGP Whole Disk Encryption verschlüsselte Laufwerke verwenden 184
Authentifizierung im PGP BootGuard-Bildschirm 184
Tastaturlayouts festlegen 188
Einzelanmeldung mit PGP Whole Disk Encryption verwenden 190
Voraussetzungen für die Verwendung der Einzelanmeldung 191
Laufwerk für die Verwendung der Einzelanmeldung verschlüsseln 191
Mehrere Benutzer und die Einzelanmeldung 192
Mit Einzelanmeldung anmelden 192
Passphrase für die Einzelanmeldung ändern 192
Dialogfeld für die Windows-Anmeldung anzeigen 193
Schutz von Laufwerken aufrechterhalten 194
Laufwerks- und Partitionsinformationen abrufen 194
Die Funktion „Umgehen“ verwenden 195
Andere Benutzer zu verschlüsselten Laufwerken oder Partitionen hinzufügen 196
Benutzer von verschlüsselten Laufwerken oder Partitionen löschen 197
Benutzer-Passphrasen ändern 197
Verschlüsselte Laufwerke oder Partitionen umschlüsseln 199
Vorgehensweise bei vergessenen Passphrasen 200
Sicherungskopien erstellen und Daten wiederherstellen 202
PGP Desktop von verschlüsselten Laufwerken oder Partitionen deinstallieren 202
Mit Wechseldatenträgern arbeiten 203
Wechseldatenträger verschlüsseln 203
Gesperrte (schreibgeschützte) Laufwerke im schreibgeschützten Modus verwenden 204
Wechseldatenträger auf anderen Systemen verwenden 205
Verschlüsselte Wechseldatenträger neu formatieren 205
PGP Whole Disk Encryption in einer von einem PGP Universal Server verwalteten Umgebung verwenden 206
PGP Whole Disk Encryption verwalten 206
Wiederherstellungs-Token erstellen 208
Wiederherstellungs-Token verwenden 209
Daten von verschlüsselten Laufwerken wiederherstellen 209
Wiederherstellungsdatenträger erstellen und verwenden 210
Mit PGP Whole Disk Encryption verschlüsselte Laufwerke entschlüsseln 212
Spezielle Sicherheitsmaßnahmen von PGP Desktop 213
Löschung der Passphrase 213
Schutz des virtuellen Speichers 214
Ruhezustand und Standbymodus 214
Schutz durch MSIM (Memory Static Ion Migration) 214
Weitere Sicherheitsaspekte 215
Windows-Vorinstallationsumgebung verwenden 215
PGP Whole Disk Encryption mit IBM Lenovo ThinkPad-Systemen verwenden 216
PGP Whole Disk Encryption mit der Microsoft Windows XP-Wiederherstellungskonsole verwenden 217

PGP Virtual Disk-Laufwerke verwenden 219

Informationen zu PGP Virtual Disk-Laufwerken 220
Neue PGP Virtual Disk-Laufwerke erstellen 221
Eigenschaften von PGP Virtual Disk-Laufwerken anzeigen 225
PGP Virtual Disk-Laufwerke suchen 225
Aktivierte PGP Virtual Disk-Laufwerke verwenden 226
- PGP Virtual Disk-Laufwerke aktivieren 226
- PGP Virtual Disk-Laufwerke deaktivieren 227
- PGP Virtual Disk-Laufwerke komprimieren 228
- PGP Virtual Disk-Laufwerke umschlüsseln 228

Mit anderen Benutzern arbeiten 230
- Konten anderer Benutzer zu einem PGP Virtual Disk-Laufwerk hinzufügen 230
- Konten anderer Benutzer von einem PGP Virtual Disk-Laufwerk löschen 231
- Konten anderer Benutzer deaktivieren und aktivieren 231
- Lese-/Schreib- und Schreibschutzstatus ändern 232
- Anderen Benutzern Administratorstatus gewähren 233

Benutzer-Passphrasen ändern 233
PGP Virtual Disk-Laufwerke löschen 234
PGP Virtual Disk-Laufwerke warten 235
- PGP Virtual Disk-Laufwerke auf einem Remoteserver aktivieren 235
- Sicherungskopien von PGP Virtual Disk-Laufwerken erstellen 235
- PGP Virtual Disk-Laufwerke austauschen 236

PGP Virtual Disk-Verschlüsselungsalgorithmen 237
Spezielle Sicherheitsfunktionen von PGP Virtual Disk 237
- Löschung der Passphrase 238
- Schutz des virtuellen Speichers 238
- Ruhezustand 238
- Schutz durch MSIM (Memory Static Ion Migration) 238
- Weitere Sicherheitsaspekte 239

Mobile Daten mit PGP Portable erstellen und darauf zugreifen 241

PGP Portable-Laufwerke erstellen 241
- PGP Portable-Laufwerk von einem Ordner erstellen 242
- PGP Portable-Laufwerk von einem USB-Wechseldatenträger erstellen 243
- PGP Portable-Laufwerke mit Lese-/Schreibzugriff oder Schreibschutz erstellen 244

Auf Daten auf einem PGP Portable-Laufwerk zugreifen 245
- Passphrase für ein PGP Portable-Laufwerk ändern 246
- PGP Portable-Laufwerk deaktivieren 247

PGP NetShare verwenden 249

Informationen zu PGP NetShare 250
- PGP NetShare-Rollen 252

PGP NetShare lizenzieren 253
Schlüssel autorisierter Benutzer 254
PGP NetShare-Administratoren (Besitzer) einrichten 254
Negativ gelistete und positiv gelistete Dateien, Ordner und Anwendungen 255
Negativ gelistete und andere Dateien, die nicht geschützt werden können 255
Vom PGP Universal Server festgelegte negativ oder positiv gelistete Ordner 256
Anwendungsbasierte Verschlüsselungslisten und Umgehungslisten für die Entschlüsselung 256
Mit geschützten Ordnern arbeiten 258
Speicherort für einen geschützten Ordner auswählen 258
Neue durch PGP NetShare geschützte Ordner erstellen 260
Dateien in durch PGP NetShare geschützten Ordnern verwenden 263
Geschützte Ordner entsperren 264
Dateien in einem geschützten Ordner ermitteln 265
Unterordner zu geschützten Ordnern hinzufügen 266
Ordnerstatus prüfen 266
Geschützte Ordner an andere Speicherorte kopieren 267
Mit PGP NetShare-Benutzern arbeiten 268
PGP NetShare-Benutzer hinzufügen 269
Rollen von Benutzern ändern 270
Benutzer aus geschützten Ordnern löschen 272
PGP NetShare-Zugriffslisten importieren 272
Mit Active Directory-Gruppen arbeiten 273
PGP NetShare für die Arbeit mit Gruppen einrichten 273
Gruppen aktualisieren 274
Durch PGP NetShare geschützte Ordner entschlüsseln 275
Ordner umschlüsseln 276
Passphrasen löschen 277
Dateien außerhalb eines geschützten Ordners schützen 277
Sicherungskopien für durch PGP NetShare geschützte Dateien erstellen 279
Mithilfe des Kontextmenüs auf PGP NetShare-Funktionen zugreifen 280
PGP NetShare in einer von einem PGP Universal Server verwalteten Umgebung 281
Auf die Eigenschaften geschützter Dateien oder Ordner zugreifen 282
PGP NetShare-Menüs in PGP Desktop verwenden 283
Menü „Datei“ 283
Menü „Bearbeiten“ 283
Menü „NetShare“ 284

PGP Zip verwenden 287

Übersicht 287
PGP Zip-Archive erstellen 288
Verschlüsselung an Empfängerschlüssel 291
Verschlüsselung mit Passphrasen 293
Selbstentschlüsselnde PGP-Archive (SDA) erstellen 296
Ein Archiv nur mit Signatur erstellen 298

PGP Zip-Archive öffnen 299
PGP Zip-SDAs öffnen 300
PGP Zip-Archive bearbeiten 301
Signierte PGP Zip-Archive verifizieren 303

Dateien mit PGP Shredder sicher löschen 305

Dateien und Ordner mit PGP Shredder sicher und endgültig löschen 305
Dateien mithilfe des PGP Shredder-Symbols auf Ihrem Desktop dauerhaft löschen 307
Dateien über PGP Desktop sicher löschen 307
Dateien aus Windows Explorer sicher löschen 307
PGP-Assistent zum sicheren Löschen von freiem Speicherplatz 308
Sicheres Löschen des freien Speicherplatzes planen 309

Schlüssel auf Smartcards und Token speichern 311

Informationen zu Smartcards und Token 312
Kompatible Smartcards 313
Smartcards erkennen 315
Smartcard-Eigenschaften untersuchen 315
Ein PGP-Schlüsselpaar auf einer Smartcard generieren 316
Öffentliche Schlüssel von Smartcards auf Schlüsselbunde kopieren 318
Schlüsselpaare vom Schlüsselbund auf eine Smartcard kopieren 319
Schlüssel von der Smartcard sicher löschen 320
Mehrere Smartcards verwenden 321
Sonder-Token 322
Aladdin eToken konfigurieren 323

PGP Desktop-Optionen festlegen 325

Zugriff auf das Dialogfeld PGP-Optionen 326
Allgemeine Optionen 327
Schlüsseloptionen 330
Hauptschlüsseloptionen 333
Messaging-Optionen 334
Proxy-Optionen 336

PGP NetShare-Optionen 340
Laufwerksoptionen 342
Notifier-Optionen 345
Erweiterte Optionen 347

Mit Kennwörtern und Passphrasen arbeiten 351

Entscheidung über die Verwendung eines Kennwortes oder einer Passphrase 352
Die Passphrasen-Qualitätsanzeige 352
Starke Passphrasen erstellen 353
Vorgehensweise bei vergessenen Passphrasen 355

PGP Desktop mit PGP Universal Server verwenden 357

Übersicht 358
Für PGP-Administratoren 359
Manuelle Bindung an einen PGP Universal Server 359

PGP Desktop mit IBM Lotus Notes verwenden 361

Informationen zur Kompatibilität von Lotus Notes und MAPI 361
PGP Desktop mit Lotus Notes verwenden 362
E-Mail-Nachrichten an Empfänger in einer Lotus Notes-Organisation senden 362
E-Mail-Nachrichten an Empfänger außerhalb einer Lotus Notes-Organisation senden 363
Bindung an einen PGP Universal Server 363
Vorbindung 363
Manuelle Bindung 364
Notes-Adressen 365
Einstellungen des Notes-Clients 365
Konfigurationsdatei „Notes.ini“ 365
Native Verschlüsselung von Lotus Notes verwenden 366

Index 369

1 Informationen zu PGP Desktop 10.0 für Windows

PGP Desktop ist eine Sicherheitslösung, die Ihre Daten mittels Kryptografie vor unbefugtem Zugriff schützt.

PGP Desktop schützt Ihre Daten, wenn sie per E-Mail oder Instant Messaging (IM) gesendet werden. Sie können eine gesamte Festplatte oder Partition (unter Windows) verschlüsseln, damit alle Daten ständig geschützt sind, oder Sie können nur einen Teil der Festplatte mithilfe eines virtuellen Laufwerks verschlüsseln, auf dem Sie Ihre vertraulichsten Daten sicher speichern können. Sie können Ihre Dateien und Ordner sicher mit anderen Benutzern im Netzwerk gemeinsam nutzen. Eine beliebige Kombination von Dateien und Ordnern kann zur einfachen Verteilung oder Sicherung in einem verschlüsselten Paket komprimiert werden. Darüber hinaus können Sie mit PGP Desktop vertrauliche Dateien sicher löschen, damit niemand mehr auf sie zugreifen kann, sowie den freien Speicherplatz auf der Festplatte überschreiben, damit keine ungesicherten Dateifragmente zurückbleiben.

Erstellen Sie mit PGP Desktop PGP-Schlüsselpaare und verwalten Sie sowohl Ihre privaten Schlüsselpaare als auch die öffentlichen Schlüssel anderer Benutzer.

Damit Sie PGP Desktop optimal nutzen können, sollten Sie mit der *PGP Desktop-Terminologie* (siehe "PGP Desktop-Grundbegriffe" auf Seite 13) vertraut sein. Außerdem ist ein Grundwissen der konventionellen Kryptografie und der Kryptografie mit öffentlichen Schlüsseln erforderlich. Weitere Informationen hierzu finden Sie unter *Konventionelle Kryptografie und Kryptografie mit öffentlichen Schlüsseln* (auf Seite 17).

In diesem Kapitel

Neuheiten bei PGP Desktop für Windows Version 10.0 2
Dieses Handbuch verwenden 5
Adressaten dieses Dokuments 7
Informationen zur Lizenzierung von PGP Desktop 7
Hilfe und Support 11

Neuheiten bei PGP Desktop für Windows Version 10.0

PGP Desktop 10.0< enthält zahlreiche Verbesserungen und die folgenden neuen Funktionen, die auf der bewährten Technologie der PGP Corporation aufbauen.

Neuerungen in PGP Desktop 10.0

Allgemein

- **Zusätzliche unterstützte Betriebssysteme**: PGP Desktop für Windows kann jetzt unter Windows 7 installiert werden.
- **Neue lokalisierte Versionen**: PGP Desktop wurde lokalisiert und kann jetzt auf Französisch (Frankreich) und Spanisch (Lateinamerika) installiert werden.
- **Unterstützung für neue Smartcards**: Sowohl für die Verwendung vor und nach dem Systemstart in PGP Desktop für Windows:
  - Axalto Cyberflex Access 32K V2-Smartcard
  - Giesecke und Devrient Sm@rtCafe Expert 3.2-PIV-Karten (Personal Identity Verification)
  - Oberthur ID-One Cosmo V5.2D-PIV-Karten
  - SafeNet iKey 2032 USB-Token
  - T-Systems Telesec NetKey 3.0- und TCOS 3.0 IEI-Karten
- **Neu gestaltete Benutzeroberfläche**: Das Hauptanwendungsfenster in PGP Desktop für Windows wurde neu gestaltet.
- **PGP Universal Server-Verbindung**: Die Ausfallsicherheit von PGP Desktop wurde erhöht, wenn die Verbindung mit dem PGP Universal Server auf einer VPN-Verbindung beruht oder anderweitig unterbrochen wird.

PGP Keys

- **Erweiterte Server-Schlüsselmodus-Schlüssel (Server Key Mode, SKM)**: SKM-Schlüssel enthalten jetzt den gesamten Schlüssel am Schlüsselbund. Darüber hinaus können SKM-Schlüssel nun für Verschlüsselungsfunktionen wie die Verschlüsselung und Entschlüsselung von Laufwerken und Dateien sowie zum Entschlüsseln von MAPI-E-Mail-Nachrichten im Offlinemodus verwendet werden.
- **Schlüsselbundspeicherort**: In PGP Desktop für Windows können Sie mithilfe von Umgebungsvariablen den Speicherort der Schlüsselbunde angeben.

- **Markierungen für die Schlüsselverwendung**: Jeder Unterschlüssel kann jetzt eigene Eigenschaften für die Schlüsselverwendung aufweisen, sodass ein Unterschlüssel ausschließlich für PGP Whole Disk Encryption und ein anderer für alle anderen PGP Desktop-Funktionen verwendet werden kann. Legen Sie die Schlüsselverwendung eines Schlüssels fest, wenn Sie einen Schlüssel nur zur Laufwerksverschlüsselung verwenden und über diesen Schlüssel keine verschlüsselten E-Mail-Nachrichten empfangen möchten.
- **Schlüsselsuche über das Universal Server-Dienstprotokoll (USP)**: Das PGP Universal-Dienstprotokoll (USP) ist ein SOAP-Protokoll, das über HTTP/HTTPS-Standardports ausgeführt wird. Dies ist jetzt der Standardmechanismus für die Schlüsselsuche. Wenn Sie in einer von einem PGP Universal Server verwalteten Umgebung arbeiten, wird PGP USP für alle Anforderungen für die Schlüsselsuche sowie für die gesamte Kommunikation zwischen dem PGP Universal Server und PGP Desktop verwendet.

PGP Messaging

- **PGP Viewer**: Verwenden Sie PGP Viewer, um ältere IMAP/POP/SMTP-E-Mail-Nachrichten zu entschlüsseln und anzuzeigen.
- **Lotus Notes**: Mit PGP Desktop ist es jetzt möglich, E-Mail-Nachrichten mit der nativen Verschlüsselung von Lotus Notes zu verschlüsseln, wenn PGP Desktop entsprechend konfiguriert und der Empfänger ein interner Notes-Benutzer ist.
- **Lotus Notes**: Mit PGP Desktop ist es jetzt möglich, E-Mail-Nachrichten im RTF-Format von Lotus Notes mit den Formaten PGP/MIME, S/MIME oder PGP-partitioniert zu verschlüsseln.
- **Lotus Notes**: PGP-Anmerkungen in Nachrichten unterstützen jetzt die regionalen Einstellungen für Datums- und Zeitstempel.
- **Hinzugefügte Microsoft Outlook-Schaltflächen**: Mithilfe von Schaltflächen können Sie Ihren Outlook-E-Mail-Nachrichten jetzt Verschlüsselung und/oder Ihre digitale Signatur manuell hinzufügen. Diese neue Funktion entspricht Gesetzen zur digitalen Signatur, die erfordern, dass die Absicht zum Signieren angezeigt wird.
- **Verbesserungen von Offline-Richtlinien**: In einer verwalteten Umgebung wird jetzt die E-Mail-Richtlinie durchgesetzt, auch wenn Sie offline und nicht mit dem PGP Universal Server verbunden sind oder wenn der Server offline ist.

PGP Portable

- PGP Portable war zuvor als eigenständige Option verfügbar und ist jetzt in PGP Desktop enthalten. PGP Portable-Laufwerke können unter Windows erstellt werden. Für diese Funktion ist eine separate Lizenz erforderlich.

PGP Whole Disk Encryption

- **Zusätzliche Smartcard-Kompatibilität**: Die folgenden neuen Karten wurden in PGP Whole Disk Encryption für Windows für die Vorstartauthentifizierung hinzugefügt: Axalto Cyberflex Access 32K V2, Marx CrypToken USB-Token, SafeNet iKey 2032 USB-Token und T-Systems T-Telesec NetKey-Smartcard.
- **Unterstützung für PIV-Karten (Personal Identity Verification)**: In PGP Whole Disk Encryption für Windows wurde Support für Benutzer mit Giesecke und Devrient Sm@rtCafe Expert 3.2- sowie Oberthur ID-One Cosmo V5.2D-PIV-Karten hinzugefügt.
- **Zusätzliche Tastaturkompatibilität (Windows)**: Insgesamt 50 Tastaturen internationaler Sprachen können jetzt zur Anmeldung bei PGP BootGuard verwendet werden. Eine Liste aller kompatiblen Tastaturen finden Sie im PGP Desktop für Windows Benutzerhandbuch oder in der Online-Hilfe.
- **Unterstützung für vollständige Laufwerksverschlüsselung unter Linux**: PGP Whole Disk Encryption für Linux bietet unter Ubuntu und Red Hat die vollständige Laufwerksverschlüsselung mit Vorstartauthentifizierung. Weitere Informationen finden Sie im PGP Whole Disk Encryption für Linux Befehlszeilenhandbuch.
- **Lokale Selbstwiederherstellung**: PGP Desktop für Windows bietet jetzt eine Möglichkeit, über den PGP BootGuard-Bildschirm auf ein verschlüsseltes Laufwerk zuzugreifen, wenn Sie die Passphrase vergessen haben. Bei entsprechender Konfiguration ist keine Unterstützung durch den Administrator erforderlich.
- **Verbesserungen bei Verwendung mit mehreren Benutzern**: In einer Umgebung, in der mehrere Benutzer auf eine Gruppe von Computern zugreifen können, kann der PGP Universal Server-Administrator eine Administratorpassphrase für PGP Whole Disk Encryption festlegen. Wenn Sie diese Passphrase im PGP BootGuard-Bildschirm auf einem System mit PGP Desktop für Windows eingeben, werden Sie zur Eingabe Ihres Windows-Kennworts aufgefordert und das Laufwerk wird entschlüsselt.
- **Verbesserungen beim Erzwingen der Verschlüsselung**: Wenn der PGP Universal Server-Administrator die Richtlinie ändert, sodass die Verschlüsselung aller Laufwerke erforderlich ist, wird beim nächsten Herunterladen der Richtlinie auf Ihr System der PGP Whole Disk Encryption-Assistent angezeigt und Sie können mit der Verschlüsselung des Laufwerks beginnen.
- **Zusätzliche Token-Unterstützung für PGP BootGuard**: Das Marx CrypToken USB-Token kann jetzt bei PGP BootGuard für PGP Desktop für Windows verwendet werden.
- **Unterstützung für erweiterte ASCII-Zeichen**: Erweiterte ASCII-Zeichen können jetzt beim Erstellen von Benutzern für PGP Whole Disk Encryption verwendet werden.

- **Kanji-Zeichen**: Kanji-Zeichen werden jetzt im PGP BootGuard-Bildschirm korrekt angezeigt.
- **Windows Server-Betriebssysteme**: PGP Whole Disk Encryption kann jetzt unter Windows Server-Betriebssystemen (Windows Server 2003 und Windows Server 2008) installiert werden. Weitere Informationen zu Systemvoraussetzungen und bewährten Methoden zum Verwenden von PGP Whole Disk Encryption auf Windows Server-Systemen finden Sie im *PGP-Wissensdatenbankartikel 1737* (http://support.pgp.com/?faq=1737).

Dieses Handbuch verwenden

In diesem Handbuch finden Sie Informationen zur Konfiguration und zur Verwendung von Komponenten in PGP Desktop. Jedes Kapitel dieses Handbuchs widmet sich einer Komponente von PGP Desktop.

„Zentral verwaltete“ und „Einzelplatz“-Benutzer

Mit einem PGP Universal-Server können die Richtlinien und Einstellungen der Komponenten von PGP Desktop gesteuert werden. Diese Funktion wird häufig in Unternehmen genutzt, die PGP-Software verwenden. PGP Desktop-Benutzer werden in dieser Konfiguration als *zentral verwaltete* Benutzer bezeichnet, da die in ihrer PGP Desktop-Software zur Verfügung stehenden Einstellungen und Richtlinien von einem PGP-Administrator vorkonfiguriert wurden und über einen PGP Universal Server zentral verwaltet werden. Wenn Sie in einer zentral verwalteten Umgebung arbeiten, gibt es in Ihrem Unternehmen u. U. spezifische Nutzungsanforderungen. Beispielsweise kann zentral verwalteten Benutzern der Versand von E-Mail-Nachrichten im Klartext gestattet oder untersagt werden oder sie müssen ihre Laufwerke mit PGP Whole Disk Encryption verschlüsseln.

Benutzer, die nicht über einen PGP Universal-Server verwaltet werden, werden als *nicht verwaltete* oder *Einzelplatz*-Benutzer bezeichnet.

In diesem Handbuch wird die Verwendung von PGP Desktop in beiden Situationen beschrieben. Verwaltete Benutzer werden während der Arbeit mit dem Produkt jedoch möglicherweise feststellen, dass einige der hier beschriebenen Einstellungen in ihren Umgebungen nicht verfügbar sind. Weitere Informationen finden Sie unter *PGP Desktop mit PGP Universal Server verwenden* (auf Seite 357).

Hinweis: Verweise auf von PGP Universal Server verwaltete Umgebungen gelten nicht für PGP Virtual Disk und PGP Virtual Disk Professional.

Vom PGP Universal Server-Administrator angepasste Funktionen

Wenn Sie PGP Desktop als „verwalteter" Benutzer in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, können einige Einstellungen vom Administrator festgelegt werden. Durch diese Einstellungen ändert sich u. U. die Anzeige bestimmter Funktionen in PGP Desktop.

- **Deaktivierte Funktionen**: Der PGP Universal Server-Administrator kann bestimmte Funktionen aktivieren oder deaktivieren. Beispielsweise kann der Administrator festlegen, dass PGP Zip-Archive oder durch PGP NetShare geschützte Ordner nicht erstellt werden können (unter Windows).

  Wenn eine Funktion deaktiviert wurde, wird das entsprechende Bedienelement auf der linken Seite nicht angezeigt und das Menü für diese Funktion steht nicht zur Verfügung. Die in diesem Handbuch enthaltenen Abbildungen entsprechen der Standardinstallation, bei der alle Funktionen aktiviert sind. Die Benutzeroberfläche von PGP Desktop sieht u. U. anders aus, wenn der Administrator die verfügbaren Funktionen angepasst hat.

- **Benutzerdefinierter BootGuard-Bildschirm**: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, hat der PGP-Administrator möglicherweise den PGP Whole Disk Encryption BootGuard-Bildschirm angepasst, damit zusätzlicher Text oder ein eigenes Bild, z. B. das Logo der Organisation, angezeigt wird. Die in diesem Handbuch enthaltenen Abbildungen entsprechen der Standardinstallation. Der Ihnen angezeigte Anmeldebildschirm sieht möglicherweise anders aus, wenn er vom Administrator angepasst wurde.

In diesem Handbuch verwendete Konventionen

Die Bezeichnungen „Hinweis", „Achtung" und „Warnung" werden folgendermaßen verwendet:

Hinweise: Hinweise enthalten zusätzliche, wichtige Informationen. Ein Hinweis lenkt Ihre Aufmerksamkeit auf wichtige Aspekte des Produkts. Durch das Lesen der Hinweise können Sie Ihre Verwendung des Produkts optimieren.

Achtung: Mit „Achtung" gekennzeichnete Vorsichtsmaßnahmen zeigen die Möglichkeit von Datenverlust oder geringfügigen Sicherheitsverletzungen an. Ein solcher Warnhinweis informiert Sie über Situationen, in denen Probleme auftreten können, sofern keine Vorsichtsmaßnahmen getroffen werden. Beachten Sie Vorsichtsmaßnahmen unbedingt.

Warnung: Warnungen zeigen die Möglichkeit schwerwiegender Datenverluste oder umfangreicher Sicherheitsverletzungen an. Eine Warnung bedeutet, dass schwerwiegende Probleme auftreten können, sofern Sie nicht geeignete Maßnahmen ergreifen. Bitten nehmen Sie Warnungen sehr ernst.

Adressaten dieses Dokuments

Dieses Dokument ist für alle Personen bestimmt, die PGP Desktop für Windows zum Schutz ihrer Daten verwenden werden.

Hinweis: Wenn Sie keine Erfahrung mit Kryptographie haben und einen Überblick über die Grundbegriffe und Konzepte von PGP Desktop wünschen, finden Sie weitere Informationen unter *Eine Einführung in die Kryptographie*. (Dieses Dokument wurde bei der Installation von PGP Desktop auf Ihrem System installiert.)

Informationen zur Lizenzierung von PGP Desktop

Die Funktionalität der PGP-Software wird mittels einer Lizenz aktiviert. Diese Lizenz legt gleichzeitig das Ablaufdatum der Software fest. Abhängig von der jeweiligen Lizenz sind einige oder alle Anwendungen der PGP Desktop-Produktfamilie aktiviert. Nachdem Sie die Lizenzinformationen eingegeben haben, müssen Sie die Software manuell oder online von der PGP Corporation autorisieren lassen.

Es gibt drei Arten von Lizenzen:

- **Bewertung**: Diese Art der Lizenz ist in der Regel zeitlich begrenzt und schließt u. U. nicht alle PGP Desktop-Funktionen ein.
- **Mietlizenz**: Diese Art der Lizenz ist in der Regel für einen Mietzeitraum von einem Jahr gültig. Während des Mietzeitraums erhalten Sie die aktuelle Version der PGP-Software sowie alle in diesem Zeitraum herausgegebenen Upgrades und Aktualisierungen.
- **Dauerlizenz**: Diese Art der Lizenz gestattet Ihnen eine zeitlich unbegrenzte Verwendung von PGP Desktop. Mit einer zusätzlich verfügbaren jährlichen Software-Versicherung, die jedes Jahr erneuert werden muss, erhalten Sie außerdem Upgrades und Aktualisierungen, die während des Versicherungszeitraums veröffentlicht werden.

PGP Desktop für Windows lizenzieren

So lizenzieren Sie PGP Desktop Führen Sie einen der folgenden Schritte aus:

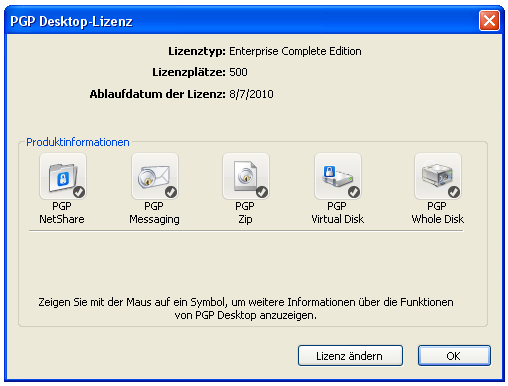
- Wenn Sie in einer verwalteten Umgebung arbeiten, verwenden Sie wahrscheinlich bereits eine lizenzierte Kopie von PGP Desktop. Überprüfen Sie die Lizenzdetails gemäß der Beschreibung unter *Lizenzdetails prüfen* (auf Seite 8). Wenn Sie Fragen haben, wenden Sie sich an den PGP-Administrator.

- Wenn Sie nicht in einer verwalteten Umgebung arbeiten oder wenn Sie ein PGP-Administrator sind, überprüfen Sie die Lizenzdetails gemäß der Beschreibung unter *Lizenzdetails prüfen* (auf Seite 8). Falls Sie Ihre Kopie von PGP Desktop autorisieren müssen, gehen Sie wie unter *PGP Desktop für Windows autorisieren* (auf Seite 9) beschrieben vor.

Lizenzdetails prüfen

So zeigen Sie die Details der PGP Desktop-Lizenz an

1. Doppelklicken Sie auf das PGP Desktop-Symbol in der Taskleiste.
2. Wählen Sie **Hilfe > Lizenz** aus. Das Dialogfeld für die PGP Desktop-Lizenz wird angezeigt.



In diesem Dialogfeld werden folgende Details angezeigt:

Element	Beschreibung
Lizenztyp	Der Name des lizenzierten Produkts.
Lizenzplätze	Die Anzahl der Plätze, für die diese Lizenz gilt.
Ablauf der Lizenz	Das Datum, an dem die Lizenz abläuft.
Produktinformationen	Die Komponenten, die bei der Lizenz aktiv sind. Zeigen Sie mit der Maus auf den Produktnamen, um Informationen zum Produkt anzuzeigen und zu erfahren, ob Sie derzeit über eine gültige Nutzungslizenz verfügen.

Hinweis: Wenn Sie Ihre Kopie von PGP Desktop nicht autorisieren, steht nur eine begrenzte Anzahl von Funktionen zur Verfügung (PGP Zip und PGP Keys).

PGP Desktop für Windows autorisieren

Wenn Sie eine neue Lizenznummer verwenden müssen oder die Lizenzautorisierung während der Konfiguration übersprungen haben, führen Sie die folgenden Schritte aus, um die Software zu aktivieren.

Hinweis: Stellen Sie zunächst sicher, dass eine Verbindung zum Internet besteht. Sollten Sie nicht über eine Internetverbindung verfügen, müssen Sie eine Anforderung für eine manuelle Autorisierung stellen.

Vorbereitung

Nach dem Kauf von PGP Desktop haben Sie eine E-Mail-Nachricht mit der Auftragsbestätigung und einer PDF-Datei als Anlage erhalten.

1. Notieren Sie Name, Organisation und Lizenznummer, die in dieser E-Mail-Nachricht angegeben sind. Diese Daten finden Sie in der PDF-Datei im Abschnitt **Important Note** (Wichtiger Hinweis). Sie benötigen diese Daten für das Lizenzierungsverfahren.

   Während der Konfiguration von PGP Desktop müssen Sie den Namen, die Organisation, die E-Mail-Adresse und die Lizenznummer eingeben, um Ihr Exemplar von PGP Desktop beim Autorisierungsserver der PGP Corporation zu autorisieren.

   Hinweis: Die Lizenznummer wird auch auf der Downloadseite des PGP-Produkts angezeigt.

   Doppelklicken Sie auf das PGP Desktop-Symbol in der Taskleiste.
2. Wählen Sie **Hilfe** > **Lizenz** aus. Das Dialogfeld für die PGP Desktop-Lizenz wird angezeigt.
3. Klicken Sie auf **Lizenz ändern**. Das Dialogfeld „PGP-Lizenzierungsassistent“ wird angezeigt.
4. Geben Sie den Namen **und die Organisation genau so an, wie sie in der PDF-Datei der E-Mail-Nachricht mit der PGP-Auftragsbestätigung aufgeführt sind. Diese Daten finden Sie in der PDF-Datei im Abschnitt Important Note** (Wichtiger Hinweis). Sollte die PDF-Datei keinen Abschnitt **Important Note** (Wichtiger Hinweis) enthalten, werden der Name und die Organisation beim ersten Autorisierungsversuch festgelegt.
5. Geben Sie die E-Mail-Adresse ein, die Sie für die Lizenzierung des Produkts verwenden möchten.
6. Geben Sie die E-Mail-Adresse zur Bestätigung erneut ein.

   Hinweis: Wenn Sie dieselbe Lizenznummer zuvor bereits autorisiert haben, müssen Sie für Name, Organisation und E-Mail-Adresse dieselben Daten eingeben wie bei der ersten Autorisierung. Falls Sie andere Informationen eingeben, schlägt die Autorisierung fehl.

7 Klicken Sie auf **Weiter**.

8 Führen Sie einen der folgenden Schritte aus:

- Geben Sie die 28-stellige Lizenznummer in die dafür vorgesehenen Felder ein (z. B. DEMO1-DEMO2-DEMO3-DEMO4-DEMO5-ABC).

Hinweis: Sie können Tippfehler vermeiden und die Autorisierung vereinfachen, indem Sie die gesamte Lizenznummer kopieren und den Mauszeiger in das erste Feld für die Lizenznummer setzen. Fügen Sie die Nummer dann ein. Die Lizenznummer wird automatisch richtig in alle sechs Felder für die Lizenznummer eingegeben.

- Wenn Sie eine einmalige 30-tägige Bewertungsversion von PGP Desktop anfordern möchten, wählen Sie **30-Tage-Bewertung von PGP Desktop anfordern** aus. Wenn Sie eine Lizenz erwerben, können Sie diese jederzeit vor Ablauf der 30-tägigen Bewertungszeit eingeben. Falls Sie keine gültige Lizenz eingeben, sind in PGP Desktop nach Ablauf der 30-tägigen Bewertungszeit nur noch die nicht lizenzierten Funktionen verfügbar.
- Wenn Sie eine PGP Desktop-Lizenz erwerben möchten, wählen Sie **Jetzt eine Lizenznummer erwerben** aus. In einem Webbrowser wird der PGP-Online-Store angezeigt.
- Wenn Sie PGP Desktop ohne Lizenz verwenden möchten, wählen Sie **Ohne Lizenz verwenden und die meisten Funktionen deaktivieren** aus. Die einzigen Funktionen von PGP Desktop, die ohne Lizenz genutzt werden können, sind PGP Zip und PGP Keys.

9 Klicken Sie auf **Weiter**, um die Autorisierung vorzunehmen.

10 Wenn die PGP-Anwendung aktiviert wurde, werden die Funktionen angezeigt, die durch die Lizenz aktiviert wurden. Klicken Sie auf **Weiter** und dann auf **Beenden**, um den Vorgang abzuschließen.

Lizenzautorisierungsfehler beheben

Fehler, die während der Autorisierung der Software ausgegeben werden, müssen entsprechend ihrer Ursache behoben werden. Lösungsvorschläge finden Sie im Abschnitt mit Informationen **zur Lizenzierung von PGP Desktop 9.x im** *PGP-Supportportal* (https://support.pgp.com).

Ablauf der Lizenz

Wenn Ihre PGP Desktop-Lizenz abgelaufen ist, wird beim Starten von PGP Desktop eine Nachricht zum Ablaufdatum der PGP-Lizenz angezeigt. Weitere Informationen zu den Auswirkungen einer abgelaufenen Lizenz auf die Funktionalität von PGP Desktop finden Sie in den folgenden Abschnitten.

PGP Desktop Email

- Ausgehende E-Mail-Nachrichten werden nicht mehr verschlüsselt gesendet.

PGP NetShare

- Der Zugriff auf durch PGP NetShare geschützte Ordner ist nicht mehr möglich, jedoch bleiben die geschützten Dateien weiterhin verschlüsselt. (Zeigen Sie die verschlüsselten Dateien an, indem Sie die Ordner und Dateien manuell entschlüsseln.)
- Neue durch PGP NetShare geschützte Ordner können nicht erstellt werden.
- Dateien, die in einen geschützten Ordner verschoben werden, werden nicht verschlüsselt.
- Schlüssel können Ordnern, die durch PGP NetShare geschützt sind, nicht hinzugefügt oder daraus entfernt werden.

PGP Virtual Disk

- Der Zugriff auf PGP Virtual Disk-Laufwerke ist nur im schreibgeschützten Modus möglich. Im schreibgeschützten Modus können Daten von einem PGP Virtual Disk-Laufwerk kopiert werden, jedoch ist das Kopieren von Daten auf ein PGP Virtual Disk-Laufwerk nicht möglich.

PGP Whole Disk Encryption

- Alle Festplatten, die mit PGP Desktop verschlüsselt wurden, werden automatisch 90 Tage nach Ablauf der Lizenz entschlüsselt.

Hilfe und Support

Informationen zu weiteren Ressourcen finden Sie in diesen Abschnitten.

Informationen zum Produkt

Sofern nicht anders angegeben, wird eine Online-Hilfe installiert, die in PGP Desktop zur Verfügung steht. Darüber hinaus sind Versionshinweise verfügbar, die kurzfristig bereitgestellte Informationen enthalten können, die nicht in der Produktdokumentation zu finden sind. Das Benutzerhandbuch und Handbücher für den Schnelleinstieg, die als Adobe Acrobat PDF-Dateien zur Verfügung gestellt werden, sind im *Supportportal der PGP Corporation* (https://support.pgp.com) zu finden.

Nach der Veröffentlichung von PGP Desktop werden zusätzliche Informationen zum Produkt zur Online-Wissensdatenbank hinzugefügt, die über die *PGP Support Knowledge Base* (https://support.pgp.com/?faq=589) verfügbar ist.

Kontaktinformationen

Kontaktaufnahme mit dem technischen Support

- Informationen zu PGP-Supportoptionen und zur Kontaktaufnahme mit dem technischen PGP-Support finden Sie auf der *Support-Homepage der PGP Corporation* (https://support.pgp.com).
- Greifen Sie auf die PGP Support Knowledge Base zu oder fordern Sie technischen PGP-Support an, indem Sie die Website des *PGP-Supportportals* (https://support.pgp.com) aufrufen. **Der Zugriff auf Teile der PGP Support Knowledge Base ist ohne Supportvertrag möglich. Wenn Sie technischen Support anfordern möchten, ist dieser jedoch erforderlich.**
- Greifen Sie auf die PGP-Supportforen über den *PGP-Support* (http://forum.pgp.com) zu. Hierbei handelt es sich um Supportforen der Benutzer-Community, die von der PGP Corporation gehostet werden.

Kontaktaufnahme mit dem Kundendienst

- Unterstützung für Bestellungen, Downloads und zur Lizenzierung erhalten Sie vom *Kundendienst der PGP Corporation* (https://pgp.custhelp.com/app/cshome).

Kontaktaufnahme mit anderen Abteilungen

- Informationen zu weiteren Möglichkeiten der Kontaktaufnahme mit der PGP Corporation finden Sie auf der *Kontaktseite der PGP Corporation* (http://www.pgp.com/about_pgp_corporation/contact/index.html).
- Allgemeine Informationen zur PGP Corporation finden Sie auf der *PGP-Website* (http://www.pgp.com).

2 PGP Desktop-Grundlagen

In diesem Abschnitt werden die Grundbegriffe von PGP Desktop beschrieben und einige wichtige Grundlagen zur Kryptographie erläutert.

In diesem Kapitel

PGP Desktop-Grundbegriffe 13
Konventionelle Kryptografie und Kryptografie mit öffentlichen Schlüsseln 17
PGP Desktop erstmals verwenden 18

PGP Desktop-Grundbegriffe

Zur optimalen Nutzung von PGP Desktop sollten Sie sich mit den Begriffen im folgenden Abschnitt vertraut machen.

PGP-Produktkomponenten

PGP Desktop und die Komponenten der Anwendung werden in der folgenden Liste beschrieben. Abhängig von der Lizenz stehen möglicherweise nicht alle Funktionen zur Verfügung. Weitere Informationen finden Sie unter *Informationen zur Lizenzierung von PGP Desktop* (siehe "PGP Desktop für Windows lizenzieren" auf Seite 7).

- **PGP Desktop**: Eine Softwareanwendung, die Daten kryptografisch vor unbefugtem Zugriff schützt. PGP Desktop ist für Mac OS X und Windows verfügbar.
    - **PGP Messaging**: Eine Funktion von PGP Desktop, die alle von Ihnen verwendeten E-Mail-Clients automatisch und transparent über von Ihnen erstellte Richtlinien unterstützt. PGP Desktop verwendet hierzu eine neue Proxy-Technologie. Die ältere Plug-in-Technologie steht ebenfalls zur Verfügung. Außerdem schützt PGP Messaging viele IM-Clients, z. B. AIM und iChat (bei beiden Benutzern muss PGP Messaging aktiviert sein).

- **PGP Whole Disk Encryption**: PGP Whole Disk Encryption ist eine Komponente von PGP Desktop, mit der gesamte Festplatten oder Partitionen (unter Windows) einschließlich des Startdatensatzes verschlüsselt werden können. Dadurch werden alle Dateien geschützt, wenn Sie sie nicht verwenden. PGP Whole Disk Encryption und PGP Virtual Disk-Laufwerke können zusammen auf einem System eingesetzt werden. Unter Windows können vollständig verschlüsselte Laufwerke mit einer Passphrase oder mit einem Schlüsselpaar auf einem USB-Token geschützt werden, um die Sicherheit zu erhöhen.
- **PGP NetShare**: Eine Funktion von PGP Desktop für Windows, mit der Sie Dateien und Ordner sicher und transparent für bestimmte Personen freigeben können. PGP NetShare-Benutzer können ihre Dateien und Ordner einfach schützen, indem sie diese in einem Ordner ablegen, der als geschützt gekennzeichnet wird.
- **PGP Keys**: Eine Funktion von PGP Desktop, die Ihnen die vollständige Kontrolle über Ihre eigenen PGP-Schlüssel und die Schlüssel von Personen gibt, mit denen Sie E-Mail-Nachrichten sicher austauschen.
- **PGP Virtual Disk-Laufwerke**: PGP Virtual Disk-Laufwerke stellen eine Funktion von PGP Desktop dar, mit der Sie einen Teil der Festplatte als verschlüsseltes virtuelles Laufwerk verwenden können. PGP Virtual Disk-Laufwerke können mit einem Schlüssel oder mit einer Passphrase geschützt werden. Sie können sogar weitere Benutzer für ein Laufwerk erstellen und dadurch autorisierten Personen den Zugriff auf das Laufwerk gestatten. Die PGP Virtual Disk-Funktion bietet sich besonders für Laptops an. Sollte der Laptop verloren gehen oder gestohlen werden, sind vertrauliche Daten, die auf dem PGP Virtual Disk-Laufwerk gespeichert sind, vor unbefugtem Zugriff geschützt.
- **PGP Shred**: Eine Funktion von PGP Desktop, mit der Sie Daten sicher vom System löschen können. Die Dateien werden von PGP Shred überschrieben und können selbst mit Software für die Datenwiederherstellung nicht wiederhergestellt werden.
- **PGP Viewer**: Mit PGP Viewer können Sie Nachrichten *außerhalb* des E-Mail-Stroms entschlüsseln, verifizieren und anzeigen.
- **PGP Zip**: Eine Funktion von PGP Desktop, mit der Sie eine beliebige Kombination von Dateien und Ordnern für die Datenübertragung oder -sicherung zu einem einzigen verschlüsselten, komprimierten Paket zusammenfassen können. Sie können ein PGP Zip-Archiv an einen PGP-Schlüssel oder an eine Passphrase verschlüsseln.

- **PGP Universal**: Ein Tool für Unternehmen, mit dem E-Mail-Nachrichten der Mitarbeiter automatisch und transparent gesichert werden. Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, werden die Messaging-Richtlinien und andere Einstellungen möglicherweise vom PGP-Administrator der Organisation gesteuert.

- **PGP Global Directory**: Ein kostenloser öffentlicher Keyserver, der von der PGP Corporation gehostet wird. Das PGP Global Directory ermöglicht den schnellen und einfachen Zugriff auf PGP-Schlüssel. Es nutzt eine Keyserver-Technologie der nächsten Generation, um die E-Mail-Adresse eines Schlüssels abzufragen (und dadurch zu prüfen, ob der Besitzer der E-Mail-Adresse den Schlüssel tatsächlich übermitteln möchte) und den Benutzern die Verwaltung ihrer Schlüssel zu ermöglichen. Durch die Verwendung des PGP Global Directory haben Sie bessere Chancen, den gültigen öffentlichen Schlüssel einer Person zu finden, der Sie sichere Nachrichten senden möchten. PGP Desktop wurde für die enge Zusammenarbeit mit dem PGP Global Directory entwickelt.

In PGP Desktop verwendete Begriffe

Bevor Sie PGP Desktop verwenden, sollten Sie sich mit den folgenden Begriffen vertraut machen.

- **Entschlüsseln:** Der Vorgang, bei dem verschlüsselte (chiffrierte) Daten wieder in lesbare Daten umgewandelt werden. Wenn Sie Daten empfangen, die von einer anderen Person mit Ihrem öffentlichen Schlüssel verschlüsselt wurden, können Sie sie mit Ihrem privaten Schlüssel entschlüsseln.
- **Verschlüsseln:** Der Vorgang, bei dem Daten chiffriert werden, damit sie für unbefugte Personen, die Zugriff auf die Daten erhalten, nicht verwendet werden können. Die Daten werden so chiffriert, dass sie bedeutungslos sind.
- **Signieren:** Der Vorgang, bei dem eine digitale Signatur mit Ihrem privaten Schlüssel auf Daten angewendet wird. Da Daten, die mit Ihrem privaten Schlüssel signiert wurden, nur durch Ihren öffentlichen Schlüssel verifiziert werden können, wird durch die Verifizierung der signierten Daten mit Ihrem öffentlichen Schlüssel belegt, dass Ihr privater Schlüssel die Daten signiert hat und die Daten daher von Ihnen stammen.
- **Verifizieren:** Der Vorgang, mit dem bewiesen wird, dass der private Schlüssel einer Person zum digitalen Signieren der Daten verwendet wurde. Dies geschieht mithilfe des öffentlichen Schlüssels der betreffenden Person. Da Daten, die mit einem privaten Schlüssel signiert wurden, nur durch den entsprechenden öffentlichen Schlüssel verifiziert werden können, beweist die Tatsache, dass ein bestimmter öffentlicher Schlüssel signierte Daten verifizieren kann, dass der Signierer wirklich der Besitzer des privaten Schlüssels ist.

- **Schlüsselpaar:** Eine Kombination aus privatem und öffentlichem Schlüssel. Wenn Sie einen PGP-Schlüssel erstellen, wird eigentlich ein Schlüsselpaar erstellt. Da Ihr Schlüsselpaar neben dem privaten und dem öffentlichen Schlüssel auch Ihren Namen und Ihre E-Mail-Adresse enthält, können Sie es sich eher als digitalen Ausweis vorstellen. Es identifiziert Sie in der digitalen Welt, so wie Sie durch Ihren Personalausweis oder Ihren Reisepass in der realen Welt ausgewiesen werden.
- **Privater Schlüssel:** Der Schlüssel, den Sie äußerst geheim halten müssen. Sie können nur mit Ihrem privaten Schlüssel Daten entschlüsseln, die mit Ihrem öffentlichen Schlüssel verschlüsselt wurden. Darüber hinaus kann nur mit Ihrem privaten Schlüssel eine digitale Signatur erstellt werden, die mit Ihrem öffentlichen Schlüssel verifiziert werden kann.

  Achtung: Geben Sie Ihren privaten Schlüssel oder dessen Passphrase niemals an andere weiter. Bewahren Sie Ihren privaten Schlüssel sicher auf.

- **Öffentlicher Schlüssel:** Der Schlüssel, den Sie an andere Personen ausgeben, damit diese Ihnen geschützte Nachrichten (Nachrichten, die nur mit Ihrem privaten Schlüssel entschlüsselt werden können) senden und Ihre digitale Signatur verifizieren können. Öffentliche Schlüssel sollten möglichst weit verbreitet werden.

  Der öffentliche und der private Schlüssel sind mathematisch betrachtet miteinander verwandt. Es ist jedoch unmöglich, aus dem öffentlichen Schlüssel einer Person deren privaten Schlüssel zu ermitteln.
- **Keyserver:** Ein Aufbewahrungsort für Schlüssel. Einige Unternehmen betreiben eigene Keyserver für die öffentlichen Schlüssel ihrer Mitarbeiter, damit diese ihre öffentlichen Schlüssel abrufen und geschützt miteinander kommunizieren können. Das *PGP Global Directory* (https://keyserver.pgp.com) ist ein kostenloser, frei zugänglicher Keyserver, der von der PGP Corporation gehostet wird.
- **Smartcards und Token:** Smartcards und Token sind tragbare Geräte, auf denen Sie ein PGP-Schlüsselpaar erstellen oder ein PGP-Schlüsselpaar kopieren können. Wenn Sie ein PGP-Schlüsselpaar auf einer Smartcard oder einem Token erstellen, wird die Sicherheit erhöht, da der Besitz der Smartcard oder des Tokens eine Voraussetzung für das Verschlüsseln, Signieren, Entschlüsseln oder Verifizieren ist. Selbst wenn eine unbefugte Person Zugriff auf Ihren Computer erlangt, bleiben Ihre verschlüsselten Daten weiterhin geschützt, da Sie Ihr PGP-Schlüsselpaar auf der Smartcard oder dem Token stets mit sich führen. Kopieren Sie das PGP-Schlüsselpaar auf eine Smartcard oder ein Token, wenn Sie es auf einem anderen System als dem Hauptsystem verwenden möchten oder wenn Sie es sichern bzw. Ihren öffentlichen Schlüssel weitergeben möchten. Smartcards und Token stehen bei der Verwendung von PGP Desktop für Mac OS X nicht als Schlüsselspeicher zur Verfügung.

Konventionelle Kryptografie und Kryptografie mit öffentlichen Schlüsseln

Konventionelle Kryptografie verwendet zum Verschlüsseln und Entschlüsseln von Daten dieselbe Passphrase. Die konventionelle Kryptografie eignet sich hervorragend für stationäre Daten, da die Verschlüsselung und Entschlüsselung sehr schnell erfolgt. Sie ist jedoch nicht besonders für Situationen geeignet, in denen Sie verschlüsselte Daten an andere Personen senden müssen, insbesondere wenn Sie mit diesen Personen noch nie Kontakt hatten.

Kryptografie mit öffentlichen Schlüsseln verwendet für das Verschlüsseln und Entschlüsseln zwei Schlüssel (ein so genanntes Schlüsselpaar). Einer der beiden Schlüssel ist Ihr privater Schlüssel, der, wie bereits der Name besagt, geheim gehalten und äußerst vertraulich behandelt werden muss. Der andere Schlüssel ist Ihr öffentlicher Schlüssel. Dieser Schlüssel kann, wie bereits der Name besagt, ohne Bedenken weitergegeben werden. Er ist sogar zur öffentlichen Weitergabe bestimmt.

Die Kryptografie mit öffentlichem Schlüssel funktioniert folgendermaßen: Angenommen, Sie und Ihre Cousine in einer anderen Stadt möchten persönliche Nachrichten austauschen. Sie beide verwenden PGP Desktop. Zunächst müssen Sie beide ein Schlüsselpaar erstellen: einen privaten Schlüssel und einen öffentlichen Schlüssel. Sie halten den privaten Schlüssel geheim und senden den öffentlichen Schlüssel an einen öffentlichen Keyserver wie das PGP Global Directory (keyserver.pgp.com), einer allgemein zugänglichen Einrichtung zum Verteilen öffentlicher Schlüssel. (Einige Unternehmen verfügen über eigene, nicht allgemein zugängliche Keyserver.)

Sobald sich die öffentlichen Schlüssel auf dem Keyserver befinden, können Sie den öffentlichen Schlüssel Ihrer Cousine von dort abrufen. Auf die gleiche Weise verfährt Ihre Cousine mit Ihrem öffentlichen Schlüssel (zum Austauschen öffentlicher Schlüssel gibt es auch andere Möglichkeiten; weitere Informationen hierzu finden Sie unter *Mit PGP-Schlüsseln arbeiten* (siehe "Mit PGP Keys arbeiten" auf Seite 43)). Dies ist wichtig, da Sie zum Senden einer verschlüsselten E-Mail-Nachricht, die nur Ihre Cousine entschlüsseln kann, die Nachricht mit dem **öffentlichen Schlüssel Ihrer Cousine verschlüsseln. Dieses Verfahren funktioniert, da eine Nachricht, die mit dem öffentlichen Schlüssel Ihrer Cousine verschlüsselt wurde, nur mit dem privaten Schlüssel Ihrer Cousine wieder entschlüsselt werden kann. Obwohl Sie im Besitz des öffentlichen Schlüssels Ihrer Cousine sind, können Sie die Nachricht nicht mehr entschlüsseln, nachdem sie mit ihrem öffentlichem Schlüssel verschlüsselt wurde. Nur mit dem privaten Schlüssel können Daten entschlüsselt werden, die zuvor mit dem entsprechenden öffentlichen Schlüssel verschlüsselt wurden.**

Der öffentliche und der private Schlüssel sind mathematisch betrachtet miteinander verwandt. Es ist jedoch nicht möglich, den privaten Schlüssel einer Person anhand des öffentlichen Schlüssels zu ermitteln.

Mehr über Kryptographie erfahren

Weitere Informationen zu Kryptographie finden Sie unter *Eine Einführung in die Kryptographie*. Diese Datei wurde bei der Installation von PGP Desktop auf Ihrem System installiert. Die Datei ist über das Startmenü zugänglich.

PGP Desktop erstmals verwenden

Die PGP Corporation empfiehlt die folgende Vorgehensweise für die ersten Schritte mit PGP Desktop:

1 **Installieren Sie PGP Desktop auf dem Computer.**

Falls Sie ein Benutzer in einem Unternehmen sind, hat der PGP-Administrator möglicherweise spezifische Installationsanleitungen für Sie vorbereitet oder das PGP-Installationsprogramm mit bestimmten Einstellungen konfiguriert. In jedem Fall stellt die Installation den ersten Schritt dar.

2 **Führen Sie die Einrichtung mit dem Einrichtungsassistenten durch.**

Nachdem Sie PGP Desktop installiert und den Computer neu gestartet haben, wird der Einrichtungsassistent geöffnet. Sie erhalten Unterstützung bei folgenden Aufgaben:

- Lizenzierung von PGP Desktop
- Erstellen eines Schlüsselpaars mit oder ohne Unterschlüsseln (falls noch kein Schlüsselpaar vorhanden ist).
- Veröffentlichen Ihres öffentlichen Schlüssels im PGP Global Directory
- Aktivieren von PGP Messaging
- Anzeigen eines Überblicks über weitere Funktionen

Wenn ein PGP-Administrator das Installationsprogramm von PGP Desktop konfiguriert hat, können mit dem Einrichtungsassistenten möglicherweise noch andere Aufgaben durchgeführt werden.

3 **Tauschen Sie öffentliche Schlüssel mit anderen Personen aus.**

Nachdem Sie ein Schlüsselpaar erstellt haben, können Sie sichere Nachrichten an andere PGP Desktop-Benutzer senden und von diesen empfangen (nachdem Sie Ihre öffentlichen Schlüssel untereinander ausgetauscht haben). Sie können auch die PGP Desktop-Funktionen für den Laufwerkschutz verwenden.

Das Austauschen öffentlicher Schlüssel ist ein wichtiger erster Schritt. Damit Sie sichere Nachrichten an andere Personen senden können, benötigen Sie eine Kopie des öffentlichen Schlüssels des Empfängers. Wenn der Empfänger mit einer sicheren Nachricht antworten möchte, benötigt er eine Kopie Ihres öffentlichen Schlüssels. Falls Sie Ihren öffentlichen Schlüssel noch nicht mit dem Einrichtungsassistenten in das PGP Global Directory übertragen haben, holen Sie dies jetzt nach. Wenn Sie nicht über den öffentlichen Schlüssel einer Person verfügen, an die Sie Nachrichten senden möchten, sollten Sie zunächst das PGP Global Directory durchsuchen. PGP Desktop übernimmt diese Aufgabe für Sie. Wenn Sie eine E-Mail-Nachricht senden, sucht die Anwendung automatisch nach den Schlüsseln anderer PGP Desktop-Benutzer und verifiziert diese. Danach wird Ihre Nachricht mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und gesendet.

4 **Überprüfen Sie die öffentlichen Schlüssel, die Sie von nicht vertrauenswürdigen Keyservern erhalten.**

Wenn Sie einen öffentlichen Schlüssel von einem nicht vertrauenswürdigen Keyserver beziehen, vergewissern Sie sich, dass er nicht verfälscht wurde und tatsächlich dem angeblichen Besitzer gehört. Vergleichen Sie zu diesem Zweck mit PGP Desktop den eindeutigen Fingerabdruck auf Ihrer Kopie des öffentlichen Schlüssels der Person mit dem Fingerabdruck auf dem Schlüssel dieser Person (z. B. indem Sie den Besitzer des Schlüssels anrufen und sich die Daten des Fingerabdrucks vorlesen lassen, sodass Sie sie vergleichen können). Schlüssel von vertrauenswürdigen Keyservern wie dem PGP Global Directory sind bereits verifiziert.

5 **Sichern Sie Ihre E-Mail-Nachrichten, Dateien und Instant Message-Sitzungen.**

Nachdem Sie Ihr Schlüsselpaar erstellt und die öffentlichen Schlüssel ausgetauscht haben, können Sie beginnen, E-Mail-Nachrichten und Dateien zu verschlüsseln, zu entschlüsseln, zu signieren und zu verifizieren. Mit der Funktion für sichere IM-Sitzungen werden automatisch eigene Schlüssel erstellt. Die Funktion kann daher verwendet werden, bevor Sie Ihr Schlüsselpaar erstellen. Die einzige Voraussetzung für sichere Sitzungen ist, dass sie mit anderen PGP Desktop-Benutzern stattfinden.

6 **Achten Sie auf Informationsfenster von PGP Desktop Notifier.**

Wenn Sie E-Mail-Nachrichten senden oder empfangen oder andere PGP Desktop-Funktionen ausführen, zeigt PGP Desktop Notifier in einer von Ihnen festgelegten Ecke des Bildschirms Informationsfenster an. In diesen Fenstern von PGP Notifier werden Aktionen gemeldet, die von PGP Desktop durchgeführt wurden bzw. durchgeführt werden. Wenn Sie sich mit dem Senden und Empfangen von Nachrichten vertraut gemacht haben, können Sie die Optionen für PGP Notifier ändern oder die Funktion deaktivieren.

7 **Nachdem Sie einige Nachrichten gesendet oder empfangen haben, prüfen Sie die Protokolle, um sicherzustellen, dass alles ordnungsgemäß funktioniert.**

Wenn Sie mehr Informationen benötigen, als von PGP Notifier angezeigt werden, finden Sie im PGP-Protokoll detaillierte Angaben zu allen Messaging-Vorgängen.

8 Ändern Sie bei Bedarf die Messaging-Richtlinien.

E-Mail-Nachrichten werden automatisch und nahtlos gesendet und empfangen, wenn die Messaging-Richtlinien von PGP Desktop ordnungsgemäß konfiguriert wurden. Wenn sich der Schlüssel des Empfängers im PGP Global Directory befindet, verwenden die Standardrichtlinien von PGP Desktop eine *opportunistische* Verschlüsselung. Das bedeutet, dass PGP Desktop die Nachricht automatisch verschlüsselt, wenn die Anwendung über alle erforderlichen Informationen verfügt (z. B. den **verifizierten** öffentlichen Schlüssel des Empfängers). Andernfalls wird die Nachricht im *Klartext* (unverschlüsselt) *gesendet. Die Standardrichtlinien von PGP Desktop ermöglichen optional auch eine erzwungene* Verschlüsselung. Dadurch **muss** eine Nachricht verschlüsselt werden, wenn in der Betreffzeile der Text „[PGP]“ angegeben wird. Wenn keine verifizierten Schlüssel gefunden werden, wird die Nachricht nicht gesendet und es wird ein Notifier-Fenster mit einer entsprechenden Meldung angezeigt.

9 Verwenden Sie die anderen Funktionen von PGP Desktop.

Sie können nicht nur die Messaging-Funktionen von PGP Desktop nutzen, sondern die Anwendung auch zum Sichern von Laufwerken verwenden:

- Verschlüsseln Sie mit **PGP Whole Disk Encryption** ein Startlaufwerk, eine Datenträgerpartition (Windows), externe Laufwerke oder USB-Flash-Laufwerke. Alle Dateien auf der Festplatte oder Partition werden gesichert und während der Verwendung entsprechend ver- und entschlüsselt. Dieser Prozess läuft für Sie völlig transparent ab.
- Erstellen Sie mit **PGP Virtual Disk** ein sicheres „virtuelles Laufwerk“. Dieses virtuelle Laufwerk kann wie ein Tresor für Ihre Dateien verwendet werden. Deaktivieren und sperren Sie das virtuelle Laufwerk mit PGP Desktop, dem Windows Explorer oder dem Finder von Mac OS X, sodass Ihre Dateien sicher sind, selbst wenn der Rest des Computers nicht gesperrt ist.
- Erstellen Sie mit **PGP Zip** komprimierte und verschlüsselte PGP Zip-Archive. Auf diese Weise können Sie Dateien effizient und sicher weitergeben oder speichern.
- Löschen Sie mit **PGP Shredder** vertrauliche Dateien, die Sie nicht mehr benötigen. PGP Shredder entfernt die Dateien vollständig von der Festplatte und sie können danach nicht mehr wiederhergestellt werden.
- Mit **PGP NetShare** können Sie Dateien und Ordner einfach und sicher für eine beliebige Anzahl von Personen freigeben und gleichzeitig höchste Zugriffskontrolle sicherstellen.

3 PGP Desktop installieren

In diesem Abschnitt wird beschrieben, wie Sie PGP Desktop auf dem Computer installieren und die ersten Schritte mit der Anwendung ausführen.

In diesem Kapitel

Installation vorbereiten.....21
PGP Desktop installieren und konfigurieren 22
Option zum Deinstallieren von PGP Desktop 26
PGP Desktop-Installation von einem Computer auf einen anderen übertragen.....27

Installation vorbereiten

In diesem Abschnitt sind die Mindestsystemanforderungen aufgeführt, die zur Installation von PGP Desktop unter Windows erforderlich sind.

Systemvoraussetzungen

Überprüfen Sie vor der Installation, ob das System folgende Mindestanforderungen erfüllt:

- Microsoft Windows 2000 (Service Pack 4),Windows Server 2003 (Service Pack 1 and 2), Windows XP Professional 32-bit (Service Pack 2 or 3), Windows XP Professional 64-bit (Service Pack 2), Windows XP Home Edition (Service Pack 2 or 3), Microsoft Windows XP Tablet PC Edition 2005 (requires attached keyboard), Windows Vista (all 32- and 64-bit editions, including Service Pack 1 and 2), Windows 7 (all 32- and 64-bit editions).

  Note: The above operating systems are supported only when all of the latest hot fixes and security patches from Microsoft have been applied.

  PGP Whole Disk Encryption (WDE) is supported on all client versions above as well as the following Windows Server versions:

  - Windows Server 2003 SP 2 (32- and 64-bit editions)
  - Windows Server 2008 SP 1 and 2 (32- and 64-bit editions)
  - Windows Server 2008 R2 (32- and 64-bit editions)

For additional system requirements and best practices information on using PGP WDE on Windows Server systems, see *PGP KB article 1737* (http://support.pgp.com/?faq=1737).

- 512 MB RAM
- 64 MB Festplattenspeicher

Informationen zu kompatibler E-Mail-, Instant Messaging- und Antivirensoftware finden Sie in den *Versionshinweisen zu PGP Desktop10.0 für Windows*.

Kompatibilität mit Citrix und Terminal-Services

PGP Desktop für Windows wurde mit folgender Software für Terminal-Services getestet:

- Citrix Presentation Server 4.0
- Citrix Metaframe XP
- Windows 2003 Terminal Services

In den genannten Umgebungen stehen die folgenden Funktionen von PGP Desktop für Windows zur Verfügung:

- Die E-Mail-Verschlüsselung wird voll unterstützt.
- PGP Zip wird voll unterstützt.
- PGP Shred wird voll unterstützt.
- PGP NetShare wird voll unterstützt.
- PGP Virtual Disk kann nicht über einen Laufwerksbuchstaben durch Citrix/TS aktiviert werden. Stattdessen wird hierfür ein Verzeichnis, der so genannte Aktivierungspunkt, auf NTFS-Laufwerken genutzt.
- PGP Whole Disk Encryption wird nicht unterstützt.
- Smartcards werden nicht unterstützt.

Informationen zur Installation von PGP Desktop auf einem Citrix-Server finden Sie im *PGP-Wissensdatenbankartikel 832* (https://support.pgp.com/?faq=832).

PGP Desktop installieren und konfigurieren

In diesem Abschnitt finden Sie Informationen zum Installieren oder Aktualisieren von PGP Desktop sowie zum Einrichtungsassistenten.

Software installieren

Hinweis: Sie müssen auf dem System über Administratorrechte verfügen, um PGP Desktop installieren zu können.

So installieren Sie PGP Desktop unter Windows

1. Suchen Sie das Installationsprogramm für PGP Desktop. Bei diesem Installationsprogramm handelt es sich um eine MSI-Datei, die Ihnen vom PGP-Administrator u. U. über das Bereitstellungsprogramm Microsoft SMS bereitgestellt wurde.
2. Doppelklicken Sie auf das Installationsprogramm für PGP Desktop.
3. Folgen Sie den Anleitungen auf dem Bildschirm.
4. Starten Sie das System neu, wenn Sie dazu aufgefordert werden.

Hinweis: Falls Sie in einer Domäne arbeiten, die durch einen PGP Universal Server geschützt ist, hat der PGP-Administrator das Installationsprogramm für PGP Desktop möglicherweise mit bestimmten Funktionen und/oder Einstellungen vorkonfiguriert. Wenn der PGP-Administrator das System für die stille Anmeldung eingerichtet hat, wird das Windows-Domänenkennwort für alle Passphrasen-Anforderungen in PGP Desktop verwendet. Wenn dies per Richtlinie festgelegt ist, kann PGP Whole Disk Encryption automatisch die Verschlüsselung des Laufwerks starten, wenn Sie das Windows-Kennwort eingeben.

Software-Upgrade

Hinweis: PGP Desktop für Windows und PGP Universal Satellite für Windows können nicht gleichzeitig auf demselben System installiert sein. Die Installationsprogramme beider Produkte erkennen, ob das jeweils andere Programm installiert ist, und brechen den Installationsvorgang ab, falls das andere Produkt gefunden wird.

Sie können von einer vorherigen Version der folgenden Produkte ein Upgrade auf PGP Desktop für Windows durchführen:

- PGP Desktop für Windows
- PGP Universal Satellite für Windows

Wenn auf dem Computer Microsoft Windows XP ausgeführt wird, können Sie lediglich ein Upgrade von PGP Desktop 8.x auf PGP Desktop 9.6 oder höher durchführen. Wenn Sie Windows 2000 verwenden, können Sie ein Upgrade von den PGP Desktop-Versionen 6.x, 7.x oder 8.x durchführen.

Wichtiger Hinweis: Wenn Sie Ihren Computer auf eine neue Betriebssystemversion aktualisieren und diese Version von PGP Desktop verwenden möchten, deinstallieren Sie zunächst alle älteren Versionen von PGP Desktop, bevor Sie das Betriebssystem aktualisieren und diese Version installieren. Sichern Sie vor der Deinstallation Ihre Schlüssel und Schlüsselbunde. Sollten Sie PGP Whole Disk Encryption verwendet haben, müssen Sie zunächst das Laufwerk entschlüsseln. Erst dann können Sie PGP Desktop deinstallieren.

Upgrade von PGP Desktop durchführen

Führen Sie einen der folgenden Schritte aus:

- **Upgrade von PGP Desktop 8.x für Windows:** Führen Sie den regulären Installationsvorgang für PGP Desktop 10.0 für Windows aus.

  PGP Desktop 8.x für Windows wird automatisch deinstalliert und PGP Desktop 10.0 für Windows wird installiert. Bestehende Schlüsselbunde sowie PGP Virtual Disk-Dateien können in der aktualisierten Version verwendet werden.

- **Upgrade von einer Version von PGP Desktop für Windows** *vor* **Version 8.0:** Deinstallieren Sie Versionen von PGP Desktop vor Version 8.0 manuell, bevor Sie mit der Installation von PGP Desktop 10.0 für Windows beginnen. Bestehende Schlüsselbunde sowie PGP Virtual Disk-Dateien können in der aktualisierten Version verwendet werden.

Upgrade von PGP Universal Satellite durchführen

Führen Sie einen der folgenden Schritte aus:

- **Upgrade von PGP Universal Satellite 1.2 für Windows oder älteren Versionen:** Führen Sie den regulären Installationsvorgang für PGP Desktop 10.0 für Windows aus.

  Bestehende Versionen von PGP Universal Satellite für Windows werden automatisch deinstalliert und PGP Desktop 10.0 für Windows wird installiert. Bestehende Einstellungen bleiben erhalten.

  Achtung: Die Installation einer beliebigen Version von PGP Universal Satellite zusätzlich zu PGP Desktop 10.0 für Windows wird nicht unterstützt. Keines der Programme wird in diesem Fall ordnungsgemäß funktionieren. Deinstallieren Sie beide Programme und installieren Sie dann ausschließlich PGP Desktop.

- **Upgrade von PGP Desktop für Windows (Version 8.x) und PGP Universal Satellite:** Führen Sie den regulären Installationsvorgang für PGP Desktop 10.0 für Windows aus.

  PGP Desktop und PGP Universal Satellite für Windows werden automatisch deinstalliert und PGP Desktop 10.0 für Windows wird installiert. Bestehende Schlüsselbunde sowie PGP Virtual Disk-Dateien können in der aktualisierten Version verwendet werden.

Auf Aktualisierungen prüfen

Wenn diese Option aktiviert ist, prüft PGP Desktop in festgelegten Intervallen automatisch, ob Softwareaktualisierungen verfügbar sind. Das Standardintervall beträgt einen Tag. Wenn eine neuere Version von PGP Desktop zum Herunterladen verfügbar ist, wird ein Benachrichtigungsbildschirm angezeigt, über den Sie die neue Version herunterladen können. Ist diese Option deaktiviert, prüft PGP Desktop nicht automatisch, ob Softwareaktualisierungen verfügbar sind. Weitere Informationen finden Sie unter *Allgemeine Optionen* (auf Seite 327).

Laden Sie die Aktualisierung herunter und installieren Sie sie, indem Sie den Aufforderungen folgen.

Für diese Option ist eine aktive Internetverbindung erforderlich.

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung verwenden, ist diese Option möglicherweise erforderlich. PGP Desktop sucht dann auf dem entsprechend zugeordneten PGP Universal Server nach Aktualisierungen.

Hinweis: Sie müssen auf dem System über Administratorrechte verfügen, um die Aktualisierung installieren zu können.

Upgrade von eigenständigen zu verwalteten Installationen von PGP Desktop

Wenn Sie PGP Desktop bisher als eigenständiges Produkt genutzt haben und nun von einem PGP Universal Server verwaltet werden, müssen Sie eine gebundene und gekennzeichnete Version von PGP Desktop auf der vorhandenen eigenständigen Version installieren. Darüber hinaus müssen Sie den Anmeldungsvorgang abschließen. Der PGP-Administrator stellt Ihnen eine Installationsdatei bereit, mit der Sie eine gebundene und gekennzeichnete Version installieren können.

Software des Betriebssystems aktualisieren

Wenn Sie den Computer auf eine neue Major Release des Betriebssystems aktualisieren (z. B. unter Windows auf Windows Vista oder unter Mac OS X von 10.4.x auf 10.5.x), müssen Sie folgende Schritte ausführen:

1. Sichern Sie vor der Deinstallation Ihre Schlüssel und Schlüsselbunde.
2. Sollten Sie PGP Whole Disk Encryption verwendet haben, müssen Sie zunächst das Laufwerk entschlüsseln. Erst dann können Sie PGP Desktop deinstallieren.
3. Deinstallieren Sie alle vorherigen Versionen von PGP Desktop, *bevor* Sie auf die neue Version des Betriebssystems aktualisieren.

4 Nach der Aktualisierung des Betriebssystems können Sie PGP Desktop neu installieren. Importieren Sie Ihre Schlüssel und Ihren Schlüsselbund und verschlüsseln Sie das Laufwerk dann bei Bedarf.

Lizenzierung von PGP Desktop

Lizenzinformationen für diese Version finden Sie in den *Versionshinweisen zu PGP Desktop.*

Einrichtungsassistenten ausführen

Wenn die Installation von PGP Desktop abgeschlossen ist, werden Sie aufgefordert, den Computer neu zu starten. Nach dem Neustart wird der Einrichtungsassistent von PGP Desktop automatisch gestartet, sobald der Windows-Desktop zu sehen ist. Der Einrichtungsassistent zeigt mehrere Bildschirme mit Fragen an. Ihre Antworten werden zur Konfiguration von PGP Desktop verwendet.

Der Einrichtungsassistent für Ihr System umfasst nur bestimmte Dialogfeld, die für Ihre Installation relevant sind. Dies hängt von verschiedenen Faktoren ab.

Mit dem Einrichtungsassistenten werden nicht alle PGP Desktop-Einstellungen konfiguriert. Wenn Sie den Einrichtungsassistenten abgeschlossen haben, können Sie die Einstellungen konfigurieren, die nicht vom Einrichtungsassistenten abgedeckt werden.

Option zum Deinstallieren von PGP Desktop

Sie können PGP Desktop mit dem Deinstallationsprogramm für PGP Desktop oder unter Verwendung der Windows-Funktion **Software** deinstallieren. Die folgende Anleitung beschreibt die Deinstallation direkt über das Deinstallationsprogramm für PGP Desktop.

Wenn Sie ein Upgrade von PGP Desktop 8.x oder höher ausführen, müssen Sie PGP Desktop **nicht** zuerst deinstallieren. Weitere Informationen finden Sie unter *Software-Upgrade* (auf Seite 23).

So deinstallieren Sie PGP Desktop

1 Klicken Sie im Menü **Start** auf **Programme > PGP > PGP Desktop deinstallieren.** Ein Bestätigungsdialogfeld wird angezeigt.

2 Klicken Sie auf **Ja**, um mit der Deinstallation fortzufahren. PGP Desktop wird vom System entfernt.

Schlüsselbunddateien sowie Dateien von PGP Virtual Disk und PGP Zip (`.pgp`) werden *nicht* vom System entfernt, falls Sie PGP Desktop zu einem späteren Zeitpunkt erneut installieren möchten.

3 Starten Sie den Computer bei Bedarf neu, um die Deinstallation abzuschließen.

Hinweis: Alternativ zur Deinstallation von PGP Desktop können Sie auch die Hintergrunddienste von PGP Desktop anhalten. Dadurch werden Ihre E-Mail- und Instant Message-Nachrichten nicht mehr durch PGP Desktop geschützt, jedoch können Sie weiterhin auf PGP Virtual Disk-Laufwerke sowie auf mit PGP Whole Disk Encryption verschlüsselte Laufwerke oder Partitionen zugreifen. Falls Sie lediglich die E-Mail- oder IM-Proxies von PGP Desktop deaktivieren möchten, verwenden Sie das Dialogfeld „PGP-Optionen“ (wählen Sie **Extras > Optionen**, klicken Sie auf die Registerkarte „Messaging“ und deaktivieren Sie die entsprechenden Optionen).

PGP Desktop-Installation von einem Computer auf einen anderen übertragen

Es ist nicht schwierig, eine PGP Desktop-Installation von einem Computer auf einen anderen zu übertragen, jedoch müssen einige wichtige Schritte erfolgreich ausgeführt werden. Der Vorgang umfasst folgende Schritte:

So übertragen Sie eine PGP Desktop-Installation auf einen anderen Computer

1 Deinstallieren Sie PGP Desktop. Wählen Sie dazu **Start > Programme > PGP > PGP Desktop deinstallieren** aus. Sie können auch die Funktion „Software“ in der Systemsteuerung von Windows verwenden. Bei älteren Versionen des Programms ist die Entfernung über die Systemsteuerung die einzige Möglichkeit, PGP Desktop zu deinstallieren.

   Beachten Sie, dass mit diesem Schritt die Schlüsselbunddateien nicht gelöscht werden.

2 Übertragen Sie die Schlüsselbunde. Kopieren Sie dazu die Schlüsselbunddateien (sowohl `pubring.pkr` als auch `secring.skr`) vom alten Computer auf eine Diskette oder einen anderen Wechseldatenträger und dann auf den neuen Computer. Der Standardspeicherort für die Schlüsselbunddateien ist C:\Dokumente und Einstellungen\<user>\Eigene Dateien\PGP\.

   Wenn PGP Desktop zuvor noch nicht auf dem neuen Computer installiert war, müssen Sie diesen Ordner erst erstellen, bevor Sie die Schlüsselbunddateien auf den Computer kopieren.

3 Installieren Sie PGP Desktop auf dem neuen Computer. Laden Sie PGP Desktop hierzu über den Downloadlink aus der ursprünglichen E-Mail-Nachricht der PGP Corporation mit der Auftragsbestätigung herunter.

4 Führen Sie während des Installationsvorgangs folgende Schritte aus:

- Geben Sie auf dem neuen Computer im Einrichtungsassistenten von PGP Desktop an, dass bereits Schlüsselbunde vorhanden sind. **Führen Sie den Speicherort auf dem neuen Computer auf, an den Sie die Schlüsselbunddateien kopiert haben.**
- Verwenden Sie dieselben Angaben für Name, Organisation und Lizenznummer, die bei der ursprünglichen Autorisierung von PGP Desktop verwendet wurden.

4 Benutzeroberfläche von PGP Desktop

In diesem Abschnitt wird die Benutzeroberfläche von PGP Desktop beschrieben.

In diesem Kapitel

Auf PGP Desktop-Funktionen zugreifen 29
Notifier-Warnungen von PGP Desktop 36
PGP-Protokoll anzeigen 41

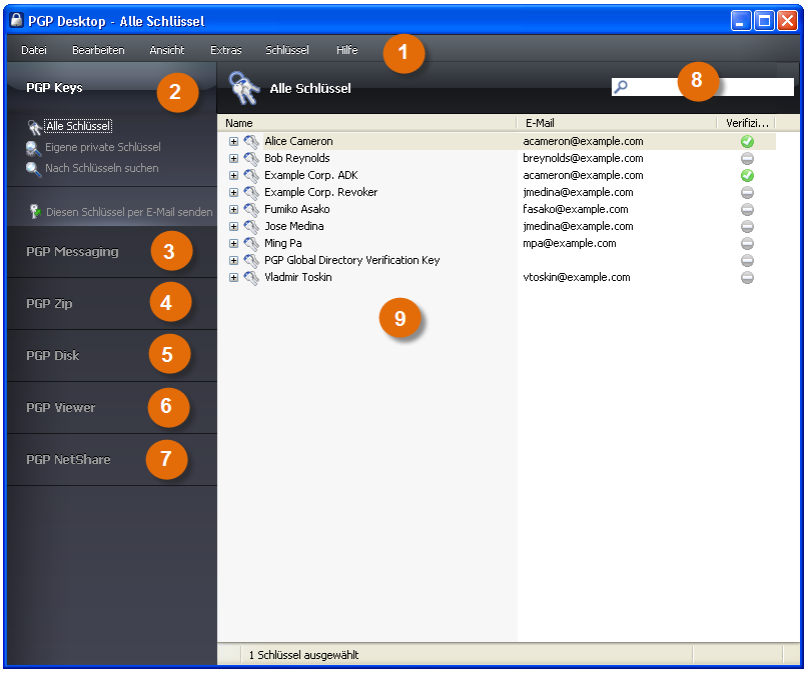
Auf PGP Desktop-Funktionen zugreifen

Es gibt vier grundlegende Möglichkeiten, auf PGP Desktop zuzugreifen:

- *Hauptfenster von PGP Desktop* (siehe "Hauptbildschirm von PGP Desktop" auf Seite 30)
- *PGP-Symbol im Infobereich der Taskleiste* (siehe "PGP-Symbol im Infobereich der Taskleiste verwenden" auf Seite 31)
- *Kontextmenüs in Windows Explorer* (siehe "Kontextmenüs in Windows Explorer verwenden" auf Seite 34)
- *Startmenü* (siehe "Startmenü verwenden" auf Seite 35)

Hauptbildschirm von PGP Desktop

Der Hauptbildschirm von PGP Desktop stellt die primäre Schnittstelle zum Produkt dar.



Der Hauptbildschirm von PGP Desktop enthält Folgendes:

1	**Menüleiste**: Ermöglicht den Zugriff auf PGP Desktop-Befehle. Die in der Menüleiste angezeigten Menüs ändern sich abhängig vom ausgewählten Bedienfeld.
2	**Bedienfeld „PGP Keys“**: Ermöglicht die Verwaltung von PGP-Schlüsseln.
3	**Bedienfeld „PGP Messaging“**: Ermöglicht die Verwaltung von PGP Messaging.
4	**Bedienfeld „PGP Zip“**: Ermöglicht die Verwaltung von PGP Zip sowie den Zugriff auf den PGP Zip-Assistenten, mit dem Sie neue PGP Zip-Archive erstellen können.
5	**Bedienfeld „PGP Disk“**: Ermöglicht die Verwaltung von PGP Disk.
6	**Bedienfeld „PGP Viewer“**: Ermöglicht das Entschlüsseln, Verifizieren und Anzeigen von Nachrichten *außerhalb* des E-Mail-Stroms.
7	**Bedienfeld „PGP NetShare“**: Ermöglicht die Verwaltung von PGP NetShare.

8	**Arbeitsbereich von PGP Desktop**: Zeigt Informationen an sowie Aktionen, die für das ausgewählte Bedienfeld durchgeführt werden können.
9	**Suchfeld „PGP Keys“:** Ermöglicht die Suche nach Schlüsseln am Schlüsselbund. Wenn Sie Text in dieses Feld eingeben, zeigt PGP Desktop Suchergebnisse entweder basierend auf Name oder E-Mail-Adresse an.

Jedes Bedienfeld kann erweitert werden, um die verfügbaren Optionen anzuzeigen, oder platzsparend ausgeblendet werden (nur die Titelleiste des Bedienfelds wird angezeigt). Sie können ein Bedienfeld erweitern, indem Sie auf die Titelleiste klicken.

Wenn ein Bedienfeld erweitert ist, ändert sich der Inhalt in Abhängigkeit davon, welche Funktionen für die durchgeführte Aktion vorgesehen sind und welche Objekte ausgewählt sind. Wenn beispielsweise das Bedienfeld „PGP Keys“ aktiv und gleichzeitig ein öffentlicher Schlüssel ausgewählt ist, werden am unteren Rand des Bedienfelds „PGP Keys“ die Optionen **E-Mail an diesen Empfänger senden** und **Diesen Schlüssel per E-Mail senden** angezeigt. Wenn ein privater Schlüssel ausgewählt ist, steht nur die Option **Diesen Schlüssel per E-Mail senden zur Verfügung. Ist kein Schlüssel ausgewählt, wird keine dieser Optionen angezeigt.**

Navigieren Sie unter Verwendung der Tabulatortaste im Hauptbildschirm von PGP Desktop. Wählen Sie mit der Leertaste oder der Eingabetaste eine Option aus.

Hinweis: Klicken Sie auf **E-Mail an diesen Empfänger senden**, um das Standard-E-Mail-Programm des Systems zu öffnen und eine neue E-Mail-Nachricht mit der Adresse des ausgewählten Schlüssels zu verfassen. Dadurch kann mühelos eine Nachricht an eine Person gesendet werden, deren Daten auf Ihrem Schlüsselbund gespeichert sind. Klicken Sie auf **Diesen Schlüssel per E-Mail senden**, um das Standard-E-Mail-Programm des Systems zu öffnen und eine neue E-Mail-Nachricht zu verfassen, an die der ausgewählte öffentliche Schlüssel als Anlage angehängt ist (die Nachricht ist zunächst nicht adressiert). Dies bietet sich an, wenn Sie Ihren öffentlichen Schlüssel oder einen öffentlichen Schlüssel an Ihrem Schlüsselbund an eine Person senden möchten, die noch nicht über diesen Schlüssel verfügt.

PGP-Symbol im Infobereich der Taskleiste verwenden

Eine Möglichkeit, auf viele der Funktionen von PGP Desktop zuzugreifen, ist das PGP-Symbol im Infobereich der Taskleiste.

Tipp: Sie können PGP Desktop öffnen, indem Sie auf das PGP-Symbol im Infobereich der Taskleiste doppelklicken.

Im PGP-Infobereich der Taskleiste wird eines von vier Symbolen angezeigt:

- **Normaler Betrieb** ( ): PGP Desktop arbeitet im Normalbetrieb. Es sind keine Passphrasen zwischengespeichert, der Nachrichten-Proxy ist aktiviert und es werden keine weiteren PGP-Vorgänge ausgeführt.
- **Passphrasen zwischengespeichert** ( ): PGP Desktop arbeitet im Normalbetrieb. Zusätzlich wurden eine oder mehrere Passphrasen für private Schlüssel zwischengespeichert. Die Zwischenspeicherung von Passphrasen ist eine optionale, zeitsparende Funktion, da eine zwischengespeicherte Passphrase nicht manuell eingegeben werden muss, wenn beispielsweise ein Schlüssel signiert werden soll. Gleichzeitig stellt die Nutzung dieser Funktion ein gewisses Sicherheitsrisiko dar. Wenn Sie Ihren Arbeitsplatz verlassen, während die Passphrase zwischengespeichert ist, kann jede andere Person PGP Desktop nutzen, ohne die gültige Passphrase zu kennen.
- **Nachrichten-Proxy deaktiviert** ( ): Die Proxyfunktion für E-Mail-Nachrichten wurde deaktiviert. Eingehende verschlüsselte Nachrichten werden nicht entschlüsselt oder verifiziert und ausgehende Nachrichten werden nicht verschlüsselt oder signiert. Sie können die Proxyfunktion für Nachrichten über das Menü des PGP-Symbols im Infobereich der Taskleiste oder über die PGP-Optionen wieder aktivieren.
- **Ausgelastet** ( ): PGP Desktop führt gerade einen Vorgang aus, beispielsweise die Verschlüsselung eines Laufwerks. Nach Abschluss des Vorgangs wird im Infobereich der Taskleiste ein anderes PGP-Symbol angezeigt, das zur jeweiligen Situation passt.

Wenn Sie mit der rechten oder linken Maustaste auf das PGP-Symbol im Infobereich der Taskleiste klicken, wird ein Menü für den Zugriff auf verschiedene Optionen angezeigt. Möglicherweise sind nicht alle Optionen verfügbar. Dies ist davon abhängig, ob Sie eine eigenständige oder eine verwaltete Installation verwenden.

- **PGP-Dienste beenden**: Hält die PGP Desktop-Dienste auf dem Computer an. Benutzen Sie diesen Befehl mit Bedacht. Sie stoppen damit die automatische Verschlüsselung und Entschlüsselung von E-Mail-Nachrichten und Instant Messaging-Sitzungen.

  Wenn Sie die PGP-Dienste beenden und dann wieder starten möchten, führen Sie entweder einen Neustart des Computers aus oder wählen Sie PGP Desktop über das Startmenü aus (**Start > Programme > PGP > PGP Desktop**).
- **Info über PGP Desktop**: Zeigt die verwendete PGP Desktop-Version sowie Lizenzinformationen an.

- **Auf Aktualisierungen prüfen**: Stellt eine Verbindung zum Aktualisierungsserver der PGP Corporation her und prüft, ob eine neuere Version von PGP Desktop zum Herunterladen verfügbar ist. Diese Option steht nur bei eigenständigen Installationen zur Verfügung.
- **Hilfe**: Öffnet die integrierte Online-Hilfe von PGP Desktop.
- **Optionen**: Öffnet das Dialogfeld mit den Optionen von PGP Desktop.
- **Notifier anzeigen**: Zeigt die letzten Meldungen für eingehende und ausgehende Nachrichten an.
- **PGP-Protokoll anzeigen**: Zeigt das PGP Desktop-Protokoll an. Das PGP Desktop-Protokoll gibt Aufschluss darüber, welche Aktionen von PGP Desktop ausgeführt werden, um Ihre Daten zu schützen.
- **PGP Viewer öffnen**: Öffnet PGP Viewer, sodass Sie E-Mail-Nachrichten außerhalb des E-Mail-Stroms entschlüsseln können.
- **PGP Desktop öffnen**: Öffnet den Hauptbildschirm von PGP Desktop. Sie können PGP Desktop auch öffnen, indem Sie im Infobereich der Taskleiste auf das PGP Desktop-Symbol *doppelklicken*.
- **Richtlinie aktualisieren**: Eine Richtlinie wird manuell vom PGP Universal Server heruntergeladen. Diese Option steht nur bei verwalteten Installationen zur Verfügung.
- **Caches löschen**: Entfernt alle zwischengespeicherten Daten, z. B. Passphrasen und zwischengespeicherte öffentliche Schlüssel, aus dem Arbeitsspeicher des Computers.

  Hinweis: Eine zwischengespeicherte Passphrase wird nicht gelöscht, wenn Sie mithilfe einer Smartcard oder eines Tokens auf einen geschützten PGP NetShare-Ordner zugegriffen und die Smartcard oder das Token entfernt haben. Definieren Sie zum Löschen einer zwischengespeicherten Passphrase einen Tastaturbefehl. Weitere Informationen finden Sie unter *Erweiterte Optionen* (auf Seite 347).

- **PGP Virtual Disk-Laufwerke deaktivieren**: Deaktiviert alle aktivierten PGP Virtual Disk-Laufwerke.
- **Aktuelles Fenster**: Wendet die Funktionen von PGP Desktop (Entschlüsseln und verifizieren, Verschlüsseln und signieren, Signieren, Verschlüsseln) auf den Inhalt des aktuellen Fensters an.
- **Zwischenablage**: Wendet die Funktionen von PGP Desktop (Entschlüsseln und verifizieren, Verschlüsseln und signieren, Signieren, Verschlüsseln) auf den Inhalt der Zwischenablage an. Darüber hinaus können Sie den Inhalt der Zwischenablage löschen oder bearbeiten.

Kontextmenüs in Windows Explorer verwenden

*Die in diesem Abschnitt beschriebenen Leistungsmerkmale finden nur dann Anwendung, wenn Sie PGP Desktop Virtual Disk Professional installiert haben. Welche Version Sie verwenden, können Sie aus dem Abschnitt unter Lizenzierung entnehmen.*Der Zugriff auf PGP Desktop-Funktionen ist auch über Kontextmenüs in Windows Explorer möglich. Öffnen Sie Windows Explorer, klicken Sie mit der rechten Maustaste auf die gewünschten Elemente und wählen Sie im Kontextmenü die Option **PGP Desktop** aus.

Über Windows Explorer können Sie abhängig von dem Element, auf das Sie mit der rechten Maustaste klicken, auf verschiedene PGP Desktop-Funktionen zugreifen:

- **Laufwerk**: Wenn Sie in Windows Explorer mit der rechten Maustaste auf ein Laufwerk des Systems klicken und im angezeigten Kontextmenü die Option „PGP Desktop“ auswählen, können Sie folgende Aktionen ausführen:
  - Freien Speicherplatz mit PGP Shred sicher löschen
- **PGP Virtual Disk**: Wenn Sie in Windows Explorer mit der rechten Maustaste auf ein PGP Virtual Disk-Laufwerk auf dem System klicken und im angezeigten Kontextmenü die Option „PGP Desktop“ auswählen, können Sie folgende Aktionen für das Laufwerk ausführen:
  - PGP Virtual Disk-Laufwerk deaktivieren
  - PGP Virtual Disk-Datei (.pgd) in Windows Explorer suchen
  - PGP Virtual Disk-Eigenschaften bearbeiten

  Wenn Sie in Windows Explorer mit der rechten Maustaste auf die PGP Virtual Disk-Datei (.pgd) eines deaktivierten Laufwerks klicken und im angezeigten Kontextmenü die Option „PGP Desktop“ auswählen, können Sie außerdem folgende Aktionen ausführen:
  - Nicht verwendeten Speicherplatz komprimieren
  - PGP Virtual Disk-Laufwerk mit PGP Shred sicher löschen (beachten Sie, dass dadurch auch alle Daten auf der Festplatte gelöscht werden)
  - PGP Virtual Disk-Laufwerk umschlüsseln
- **Ordner**: Wenn Sie in Windows Explorer mit der rechten Maustaste auf einen Ordner klicken und im angezeigten Kontextmenü die Option „PGP Desktop“ auswählen, können Sie folgende Aktionen für den Ordner ausführen:
  - Zu neuem PGP Zip-Archiv hinzufügen
  - Selbstentschlüsselndes Archiv (SDA) mit dem Inhalt des Ordners erstellen
  - Mit einem Schlüssel oder einer Passphrase sichern
  - Entschlüsseln und verifizieren

- Zu PGP NetShare hinzufügen
- Sicher löschen

- **Datei**: Wenn Sie in Windows Explorer mit der rechten Maustaste auf eine Datei klicken und im angezeigten Kontextmenü die Option „PGP Desktop“ auswählen, können Sie abhängig von der Art der Datei folgende Aktionen ausführen:
  - Wenn Sie eine nicht verschlüsselte Datei auswählen, können Sie diese mit einem Schlüssel oder einer Passphrase sichern oder Sie können sie signieren, sicher löschen oder ein selbstentschlüsselndes Archiv (SDA) erstellen.
  - Wenn Sie eine verschlüsselte Datei auswählen, können Sie diese entschlüsseln und verifizieren oder sicher löschen.
  - Wenn Sie ein deaktiviertes PGP Virtual Disk-Laufwerk (`.pgd`) auswählen, können Sie dieses aktivieren oder bearbeiten. Wenn Sie ein aktiviertes Laufwerk auswählen, können Sie es deaktivieren.
  - Wenn Sie eine PGP Zip-Datei (.pgp) auswählen, können Sie diese entschlüsseln und verifizieren, anzeigen oder sicher löschen.
  - Wenn Sie eine PGP-Schlüsseldatei (`.asc`) auswählen, können Sie diese entschlüsseln und verifizieren oder sicher löschen. Wenn Sie die Option zum Entschlüsseln und Verifizieren auswählen, besteht die Möglichkeit, die Datei zu importieren.
  - Wenn Sie eine öffentliche oder private PGP-Schlüsselbunddatei (.pkr bzw. .skr) auswählen, können Sie die darin enthaltenen Schlüssel Ihrem Schlüsselbund hinzufügen oder die Datei sicher löschen.

Startmenü verwenden

Sie können über das Windows-Startmenü auf PGP Desktop zugreifen. Wählen Sie hierzu **Start > Programme > PGP** aus.

Über das Startmenü haben Sie Zugriff auf folgende Komponenten:

- Die PGP Desktop-Dokumentation in englischer sowie anderen unterstützten Sprachen
- Die PGP Desktop-Anwendung
- Option zum Deinstallieren von PGP Desktop

Notifier-Warnungen von PGP Desktop

Die Notifier-Funktion von PGP Desktop zeigt in einem kleinen Fenster Informationen zum Status von ein- und ausgehenden E-Mail-Nachrichten sowie zu Instant Messaging-Sitzungen an.

Hinweis: Die Notifier-Funktion von PGP Desktop meldet auch den Status von PGP Whole Disk Encryption und PGP NetShare auf dem Computer. Weitere Informationen finden Sie unter *PGP Desktop Notifier für Laufwerksfunktionen* (auf Seite 39).

PGP Desktop Notifier für Messaging

PGP Desktop Notifier für Messaging bietet folgende Funktionen:

- Anzeigen von Benachrichtigungen, ob eingehende E-Mail-Nachrichten ordnungsgemäß entschlüsselt und/oder signiert wurden
- Anzeigen von Benachrichtigungen, ob ausgehende E-Mail-Nachrichten ordnungsgemäß verschlüsselt und/oder signiert werden
- Verhindern des Sendens von E-Mail-Nachrichten, wenn die Verschlüsselungsoptionen nicht Ihren Wünschen entsprechen
- Anzeigen einer kurzen Übersicht mit Absender, Betreff und Verschlüsselungsschlüssel einer E-Mail-Nachricht
- Überprüfen des Status der in der aktuellen Windows-Sitzung bereits eingegangenen oder ausgegangenen E-Mail-Nachrichten
- Anzeigen von Benachrichtigungen, ob eine Chat-Sitzung mit einem anderen Benutzer von PGP Desktop geschützt wird

Mit der Notifier-Funktion von PGP Desktop können Sie alle oder bestimmte eingehende E-Mail-Nachrichten überwachen sowie das Senden aller oder bestimmter ausgehender E-Mail-Nachrichten genau steuern. Die Entscheidung liegt bei Ihnen. Sie können verschiedene Notifier-Optionen festlegen oder die Notifier-Funktion von PGP Desktop bei Bedarf vollständig deaktivieren.

Beachten Sie bei der Arbeit mit der Notifier-Funktion von PGP Desktop folgende zusätzliche Hinweise:

- Navigieren Sie bei Meldungen zu Nachrichten mit den Pfeilschaltflächen nach links und rechts in der rechten oberen Ecke des Notifier-Fensters vorwärts oder rückwärts durch die Notifier-Meldungen. Auf diese Weise können Sie die Meldungen überprüfen, die vor oder nach der aktuell angezeigten Meldung eingegangen sind.

- Die Notifier-Meldungsfenster werden zunächst teilweise transparent angezeigt, damit der Bildschirminhalt nicht verdeckt wird. Sie werden undurchsichtig angezeigt, wenn Sie mit dem Mauszeiger über das Fenster fahren, und werden wieder transparent, wenn Sie den Mauszeiger aus dem Meldungsfenster entfernen.
- Sofern der Mauszeiger nicht über einer Notifier-Meldung platziert ist, wird diese Meldung vier Sekunden lang angezeigt. Diese Standardeinstellung kann in den Notifier-Optionen geändert werden. Wenn Sie mehr Zeit zum Lesen einer Meldung benötigen, zeigen Sie mit dem Mauszeiger auf die Meldung, damit sie eingeblendet bleibt.
- Wenn Sie eine Notifier-Meldung verpassen oder eine ältere Meldung noch einmal ansehen möchten, gehen Sie wie folgt vor:
  - Windows: Klicken Sie im PGP-Symbol im Infobereich der Taskleiste auf **Notifier anzeigen.**
  - Mac OS X: Klicken Sie in der Menüleiste von Mac OS X auf das PGP Desktop-Symbol und wählen Sie **Notifier anzeigen** aus.
- Schließen Sie eine Notifier-Meldung, indem Sie auf das **X** klicken (oben rechts in der Meldung bei Windows-Systemen und oben links bei Mac OS X-Systemen).

Weitere Informationen zum Einrichten der Notifier-Optionen von PGP Desktop finden Sie unter *Notifier-Optionen* (auf Seite 345).

PGP Desktop Notifier-Meldungen zu eingehenden Nachrichten

Meldungen zu eingehenden E-Mail-Nachrichten können Sie entnehmen, ob die E-Mail-Nachricht entschlüsselt und verifiziert wurde oder mit einem nicht verifizierten oder unbekannten Schlüssel entschlüsselt oder signiert wurde.

PGP Desktop Notifier-Meldungen zu ausgehenden Nachrichten

Für eine einfache Benachrichtigung können Sie wählen, dass beim Senden von E-Mail-Nachrichten kurz eine PGP Desktop Notifier-Meldung angezeigt wird. Diese Meldung kann für alle E-Mail-Nachrichten oder nur für bestimmte E-Mail-Nachrichten erfolgen, die bestimmte Kriterien erfüllen.

Darüber hinaus können Sie PGP Desktop so konfigurieren, dass im Notifier-Fenster die Schaltflächen **Blockieren** und **Senden** angezeigt werden.

So verwalten Sie ausgehende E-Mail-Nachrichten mit dieser Notifier-Meldung

1. Gehen Sie im Notifier-Fenster für ausgehende PGP-Nachrichten folgendermaßen vor:

- Klicken Sie auf **Blockieren**, wenn die Nachricht nicht gesendet werden soll. Beachten Sie, dass dadurch nur diese ausgehende E-Mail-Nachricht blockiert wird. Künftige E-Mail-Nachrichten an diesen Absender können gesendet werden.
- Klicken Sie auf **Senden**, wenn diese Nachricht gesendet werden soll, obwohl der Schlüssel des Empfängers nicht gefunden wurde.
- Wenn die Verarbeitung einer Nachricht verzögert werden soll, lassen Sie den Mauszeiger auf dem Notifier-Fenster. Wenn Sie den Mauszeiger vom Notifier-Fenster entfernen, wird die Nachricht entsprechend der Standardregel verarbeitet.
- Mit der Notifier-Option **Ausgehende E-Mail-Nachrichten verzögern um** legen Sie fest, nach wie vielen Sekunden eine E-Mail-Nachricht gesendet wird, wenn Sie keine Aktion durchführen. Die verbleibende Zeit wird angezeigt.

2 Wenn Sie weitere Informationen anzeigen möchten, z. B. zu Aktion, Empfänger, Richtlinie oder Signierschlüssel, klicken Sie auf **Mehr**.

Es ist nicht zwingend erforderlich, diese zusätzlichen Informationen anzuzeigen. Blenden Sie diese Informationen wieder aus, indem Sie auf **Weniger** klicken.

PGP Desktop Notifier-Meldungen zu ausgehenden Nachrichten für Offline-Richtlinien

Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, hat der Administrator u. U. festgelegt, welche Aktionen bei ausgehenden Nachrichten durchgeführt werden, wenn der PGP Universal Server nicht verfügbar ist. Die Notifier-Meldung zu ausgehenden Nachrichten zeigt Folgendes an:

- Der PGP Universal Server ist nicht verfügbar und per Richtlinie werden alle Nachrichten blockiert. E-Mail-Nachrichten bleiben im Postausgang und werden gesendet, wenn eine Verbindung zum PGP Universal Server hergestellt werden kann.
- Der PGP Universal Server ist nicht verfügbar und per Richtlinie werden alle Nachrichten als Klartext gesendet.
- Der PGP Universal Server ist nicht verfügbar und per Richtlinie wurde einer lokalen Richtlinie Vorrang eingeräumt.

In den letzten beiden Fällen können Sie die ausgehende Nachricht, wie jede andere ausgehende Nachricht, senden oder blockieren.

PGP Notifier für Instant Messaging

Wenn PGP Desktop auf dem Computer installiert ist und Sie die Notifier-Funktion für Instant Messaging aktiviert haben (in den PGP Desktop-Einstellungen auf der Registerkarte **Benachrichtigungen**), werden Sie in Notifier-Meldungen von PGP Desktop darüber informiert, wenn AIM-Sitzungen (AOL Instant Messenger) mit anderen PGP Desktop-Benutzern geschützt sind.

Wenn Sie die Funktion für sicheres Instant Messaging verwenden, wird beim Anmelden im Instant Messaging-Programm eine Notifier-Meldung angezeigt, dass der Chat sicher ist. Zudem wird in den meisten AIM-kompatiblen Instant Messaging-Clients ein Schlosssymbol neben Ihrem Buddy-Namen angezeigt.

Wenn Sie sich vom Instant Messaging-Programm abmelden, werden Sie in einer abschließenden Notifier-Meldung darüber informiert, dass die sichere Sitzung beendet wurde.

Weitere Informationen zur Konfiguration und Verwendung der Funktion für sichere Instant Message-Chats finden Sie unter IM-Nachrichten sichern.

PGP Desktop Notifier für Laufwerksfunktionen

Mit PGP Desktop Notifier für Laufwerksfunktionen bleiben Sie bei der Arbeit mit PGP NetShare und PGP Whole Disk Encryption auf dem Laufenden.

Hinweis: Die Notifier-Funktion von PGP Desktop zeigt auch den Status von ein- und ausgehenden E-Mail-Nachrichten auf dem Computer an. Weitere Informationen finden Sie unter *PGP Desktop Notifier für Messaging* (auf Seite 36).

PGP NetShare

Wenn Sie die Notifier-Funktion von PGP Desktop zusammen mit PGP NetShare verwenden, werden Sie über Folgendes informiert:

- An freigegebenen Ordnern vorgenommene Aktionen
- Speicherort des betreffenden Ordners
- Name des betreffenden Ordners
- Name des Benutzers, der die Aktion durchgeführt hat

PGP Whole Disk Encryption

Wenn Sie die Notifier-Funktion von PGP Desktop zusammen mit PGP Whole Disk Encryption verwenden, werden Sie über Folgendes informiert:

- Das zu verschlüsselnde Laufwerk

- Größe und Typ des Laufwerks
- Status des Verschlüsselungsvorgangs

Notifier-Meldungen aktivieren oder deaktivieren

So aktivieren oder deaktivieren Sie Notifier-Meldungen

1. Öffnen Sie PGP Desktop und wählen Sie **Extras > Optionen** aus.
2. Klicken Sie auf die Registerkarte „Notifier“.
3. Wählen Sie unter **Verwendung** die Option **PGP Notifier verwenden** aus, wenn Sie die Funktion aktivieren möchten, und legen Sie den Speicherort fest. PGP Desktop-Benachrichtigungen können in einer der vier Ecken des Bildschirms angezeigt werden (**Unten rechts**, **Unten links**, **Oben rechts** oder **Oben links**). Wählen Sie die Ecke aus, in der die PGP Desktop-Benachrichtigungen angezeigt werden sollen. Die Standardposition ist **Unten rechts**.
4. Wenn Sie PGP Desktop Messaging verwenden und die Notifier-Meldungen von PGP Desktop eingeblendet werden sollen, in denen der Verschlüsselungs- oder Signierstatus beim Senden von E-Mail-Nachrichten angezeigt wird, aktivieren Sie das Kontrollkästchen **Beim Verarbeiten ausgehender E-Mail-Nachrichten benachrichtigen**. Deaktivieren Sie dieses Kontrollkästchen, wenn Sie beim Senden von E-Mail-Nachrichten keine PGP Desktop-Benachrichtigungen wünschen.
5. PGP Desktop sucht nach einem öffentlichen Schlüssel für jeden Empfänger der von Ihnen gesendeten E-Mail-Nachrichten. Wenn für einen Empfänger kein öffentlicher Schlüssel gefunden werden kann, wird die betreffende E-Mail-Nachricht standardmäßig als Klartext (ohne Verschlüsselung) gesendet. Wählen Sie die Option **Vor dem Senden von E-Mail-Nachrichten nachfragen, wenn der Schlüssel des Empfängers nicht gefunden wird** aus, wenn Sie informiert werden möchten, wenn ein Schlüssel nicht gefunden wird. Sie erhalten dann die Möglichkeit, die E-Mail-Nachricht zu blockieren, sodass sie nicht gesendet wird. Legen Sie dann folgende Optionen fest:
   - **Vor dem Senden von E-Mail-Nachrichten immer nachfragen:** Aktivieren Sie dieses Kontrollkästchen, wenn Sie jede E-Mail-Nachricht vor dem Versand bestätigen möchten. Sie können den Verschlüsselungsstatus im Notifier-Fenster überprüfen und dann entscheiden, ob die E-Mail-Nachricht gesendet oder blockiert werden soll.

- **Ausgehende E-Mail-Nachricht zum Bestätigen um n Sekunden verzögern** (wobei *n* für eine Zahl zwischen 1 und 30 steht; der Standardwert beträgt 4 Sekunden): Ändern Sie die Verzögerungszeit für ausgehende Nachrichten sowie die Zeit für die Anzeige des Notifier-Fensters von PGP Desktop, indem Sie die Pfeiltasten nach oben und nach unten verwenden. Innerhalb der Verzögerungszeit können Sie die Notifier-Meldung von PGP Desktop überprüfen.

(Weitere Informationen zu den Einstellungen für die Standardrichtlinien von PGP Desktop finden Sie unter *Dienste und Richtlinien* (auf Seite 103).)

6 Geben Sie für eingehende E-Mail-Nachrichten an, wie deren Status beim Empfang angezeigt werden soll. Wählen Sie unter **Benachrichtigungen für eingehende E-Mail-Nachrichten anzeigen** eine der folgenden Optionen aus:

- **Beim Empfang sicherer E-Mail-Nachrichten**: Beim Empfang sicherer E-Mail-Nachrichten wird ein Notifier-Fenster angezeigt. Dieses Fenster enthält den Absender der E-Mail-Nachricht, den Betreff, den Verschlüsselungs- sowie den Verifizierungsstatus und die E-Mail-Adresse des Absenders.
- **Nur beim Fehlschlagen der Nachrichtenüberprüfung**: Eine Notifier-Meldung wird nur dann für eingehende E-Mail-Nachrichten angezeigt, wenn PGP Desktop die Signatur der eingehenden E-Mail-Nachricht nicht verifizieren kann.
- **Nie**: Wählen Sie diese Option aus, wenn beim Empfang von E-Mail-Nachrichten keine Notifier-Meldung angezeigt werden soll. Diese Option wirkt sich nicht auf Notifier-Meldungen für ausgehende E-Mail-Nachrichten aus.

7 Wenn zu Beginn und bei Beendigung eines sicheren Instant Messaging-Chats kurz eine Notifier-Meldung von PGP Desktop angezeigt werden soll, aktivieren Sie das Kontrollkästchen **Über Status verschlüsselter PGP-IM-Sitzungen benachrichtigen**.

PGP-Protokoll anzeigen

Das PGP-Protokoll gibt Aufschluss darüber, welche Aktionen von PGP Desktop ausgeführt werden, um Ihre Daten zu schützen.

So zeigen Sie das PGP-Protokoll an

1 Damit Protokolle angezeigt werden können, müssen Sie die Protokollfunktion aktivieren. Klicken Sie dazu in PGP Desktop auf **Extras > Protokollierung aktivieren**.

2 Führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf das PGP Desktop-Symbol in der Taskleiste und klicken Sie im Kontextmenü auf **PGP-Protokoll anzeigen**. Das PGP-Protokoll wird in einem neuen Fenster geöffnet.
- Klicken Sie in PGP Desktop auf **Extras > Protokoll anzeigen**. Das PGP-Protokoll wird in einem neuen Fenster geöffnet.
- Klicken Sie in PGP Desktop auf das Bedienfeld „PGP Messaging“ und wählen Sie **PGP-Protokoll** aus. Daraufhin wird das PGP-Protokoll im Anwendungsfenster angezeigt.

3 Führen Sie folgende Schritte aus, um die Anzeigeoptionen zu ändern oder Filter für bestimmte Protokollinformationen zu verwenden:

- Klicken Sie auf den Pfeil für das Menü **Protokoll anzeigen für**, um den Zeitraum auszuwählen, für den Protokolle angezeigt werden sollen.
- Klicken Sie auf den Pfeil für das Menü **Thema anzeigen**, um die Arten der Protokolle auszuwählen, die Sie anzeigen möchten. Sie haben die Wahl zwischen **Alle**, **PGP**, **E-Mail**, **IM**, **Whole Disk**, **NetShare**, **Zip/SDA** und **Virtual Disk**.
- Klicken Sie auf den Pfeil für das Menü **Stufe anzeigen**, um den Mindestschweregrad der Protokolleinträge auszuwählen, die Sie anzeigen möchten. Sie haben die Wahl zwischen **Fehler**, **Warnung**, **Info** und **Ausführlich**.

  Wenn Sie Protokolle anzeigen möchten, die mit der Option **Ausführlich** aufgezeichnet wurden, muss das Anzeigefenster für das PGP-Protokoll geöffnet bleiben. Wenn Sie das Fenster schließen, kehrt das System zur Standardprotokollierungsstufe **Info** zurück. Beachten Sie, dass die Option **Ausführlich** zu sehr großen Protokolldateien führen kann.

4 Nach Abschluss der Anzeige des Protokolls:

- Klicken Sie auf **Speichern**, um eine Kopie des PGP-Protokolls zu speichern.
- Klicken Sie auf **Sicher löschen**, wenn Sie die Einträge im PGP-Protokoll entfernen möchten.
- Klicken Sie auf **Schließen**, um das PGP-Protokollfenster zu schließen.

5 Mit PGP Keys arbeiten

PGP Keys ist eine Funktion von PGP Desktop, mit der Sie eigene PGP-Schlüsselpaare und öffentliche Schlüssel anderer PGP Desktop-Benutzer erstellen und verwalten können.

In diesem Abschnitt wird beschrieben, wie Sie Schlüssel anzeigen, ein Schlüsselpaar erstellen, Ihren öffentlichen Schlüssel verteilen, die öffentlichen Schlüssel anderer Personen abrufen und mit Keyservern arbeiten.

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung verwenden, hat Ihr PGP Universal Server-Administrator ggf. bestimmte Funktionen deaktiviert. Ist eine Funktion deaktiviert, wird das Bedienelement auf der linken Seite nicht angezeigt und das Menü oder andere auf diese Funktion zutreffenden Optionen sind nicht verfügbar. Die in diesem Handbuch enthaltenen Abbildungen entsprechen der Standardinstallation, bei der alle Funktionen aktiviert sind. Wenn Ihr PGP Universal Server-Administrator diese Funktion deaktiviert hat, ist dieser Abschnitt für Sie nicht relevant.

In diesem Kapitel

Schlüssel anzeigen....43
Schlüsselpaare erstellen....44
Privaten Schlüssel schützen....48
Öffentliche Schlüssel verteilen....51
Öffentliche Schlüssel anderer Personen erhalten....54
Mit Keyservern arbeiten....56
Hauptschlüssel verwenden....58

Schlüssel anzeigen

Wenn Sie Schlüssel am lokalen Schlüsselbund anzeigen möchten, öffnen Sie PGP Desktop und klicken Sie auf das Bedienfeld „PGP Keys“. Klicken Sie dann auf:

- **Alle Schlüssel**: Zeigt alle PGP-Schlüssel an Ihren Schlüsselbunden an.
- **Eigene private Schlüssel**: Zeigt nur die privaten Schlüssel an Ihren Schlüsselbunden an.

- **Nach Schlüsseln suchen**: Ermöglicht Ihnen die Suche nach Schlüsseln an Ihren Schlüsselbunden auf der Basis Ihrer Suchkriterien.
- **Smartcard-Schlüssel**: Wenn auf dem System eine Smartcard vorhanden ist, steht auch diese Option zur Verfügung.

Einige der häufiger verwendeten Aufgaben stehen im Bedienfeld von PGP Keys oder im Arbeitsbereich zur Verfügung. Hierbei handelt es sich um Folgende:

- Wenn ein öffentlicher Schlüssel in einer Ansicht der PGP-Schlüssel an Ihren Schlüsselbunden ausgewählt ist, wird die Option **E-Mail an diesen Empfänger senden** im Bedienfeld von PGP Keys eingeblendet.
- Wenn Sie eine Suche durchführen und einen öffentlichen Schlüssel auswählen, der bei der Suche gefunden wurde und der sich nicht an Ihren lokalen Schlüsselbunden befindet, wird im Bedienfeld von PGP Keys die Option **Zu eigenem Schlüsselbund hinzufügen** angezeigt.
- Wenn Sie die Eigenschaften eines im Arbeitsbereich aufgeführten Schlüssels anzeigen möchten, können Sie auf einen Teil des aufgeführten Schlüssels doppelklicken, um das Dialogfeld „Eigenschaften“ für diesen Schlüssel zu öffnen.

Wenn Sie eine Suche durchführen, wird im Bedienfeld von PGP Keys die Option **Diese Schlüsselsuche speichern** angezeigt, sodass Sie die Ergebnisse zur späteren Verwendung speichern können.

Schlüsselpaare erstellen

Sie haben wahrscheinlich bereits ein PGP-Schlüsselpaar für den persönlichen Gebrauch erstellt, entweder mit dem Einrichtungsassistenten von PGP Desktop oder mit einer früheren Version von PGP Desktop. Ist dies nicht der Fall, müssen Sie es jetzt nachholen. Für fast alle Aktionen in PGP Desktop ist ein Schlüsselpaar erforderlich.

Achtung: Es ist nicht empfehlenswert, für sich selbst immer neue Schlüssel zu erstellen. Ein PGP-Schlüsselpaar ist wie ein digitaler Personalausweis oder Pass. Wenn Sie zu viele davon erstellen, verwirren Sie am Ende nicht nur sich selbst, sondern auch die Personen, die Ihnen verschlüsselte Nachrichten senden möchten. Es ist am besten, wenn Sie nur über einen einzigen Schlüssel verfügen, der alle von Ihnen verwendeten E-Mail-Adressen enthält. Das PGP Global Directory veröffentlicht jeweils nur ein Schlüsselpaar pro E-Mail-Adresse.

Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, ist die Funktion zum Erstellen von Schlüsselpaaren möglicherweise deaktiviert.

So erstellen Sie ein PGP-Schlüsselpaar

1 Achten Sie darauf, dass das Bedienfeld „PGP Keys“ ausgewählt ist.

2 Klicken Sie auf **Datei > Neuer PGP-Schlüssel** oder drücken Sie Strg+N. Der erste Bildschirm des Assistenten für die Erstellung eines PGP-Schlüssels wird angezeigt.

3 Lesen Sie die Informationen auf diesem Bildschirm.

4 Wenn Sie das neue PGP-Schlüsselpaar auf einem Token oder einer Smartcard erstellen möchten, stellen Sie sicher, dass das Token bzw. die Smartcard an das System angeschlossen ist und markieren Sie die Option **Schlüssel auf Token erstellen: [Name der Smartcard oder des Tokens im System]**. Weitere Informationen zu Smartcards und Token finden Sie unter *Schlüssel auf Smartcards oder Token speichern* (siehe "Schlüssel auf Smartcards und Token speichern" auf Seite 311).

5 Klicken Sie auf **Weiter**. Der Bildschirm „Zuweisung von Name und E-Mail“ wird angezeigt.

6 Geben Sie im Feld **Vollständiger Name** Ihren tatsächlichen Namen und im Feld **Primäre E-Mail-Adresse** Ihre richtige E-Mail-Adresse ein. Es ist nicht zwingend erforderlich, Ihren tatsächlichen Namen oder Ihre E-Mail-Adresse einzugeben. Wenn Sie jedoch Ihren tatsächlichen Namen und Ihre richtige E-Mail-Adresse verwenden, können Sie von anderen Personen leichter als Eigentümer Ihres öffentlichen Schlüssels identifiziert werden. Ihre richtige E-Mail-Adresse ist ebenfalls erforderlich, wenn Sie Ihren öffentlichen Schlüssel in das PGP Global Directory hochladen (das ihn auf einfache Weise für andere PGP Desktop-Benutzer verfügbar macht).

7 Falls Sie dem Schlüssel, den Sie erstellen, weitere E-Mail-Adressen hinzufügen möchten, klicken Sie auf **Mehr** und geben Sie die Adressen in die entsprechenden Felder ein.

8 Falls Sie erweiterte Einstellungen für den Schlüssel angeben möchten, den Sie erstellen, klicken Sie auf **Erweitert**. Das Dialogfeld „Erweiterte Schlüsseleinstellungen“ wird angezeigt. In diesem Dialogfeld können Sie den Typ, die Größe, die Gültigkeitsdauer und andere Einstellungen für den Schlüssel festlegen.

9 Wählen Sie Einstellungen für die folgenden Punkte aus:

- **Schlüsseltyp**: Wählen Sie zwischen Diffie-Hellman/DSS und RSA.
- **Separaten Signatur-Unterschlüssel erstellen**: Aktivieren Sie dieses Kontrollkästchen, wenn Sie einen separaten Unterschlüssel zum Signieren benötigen. Zusammen mit dem neuen Schlüsselpaar wird ein separater Signatur-Unterschlüssel erstellt. Nachdem der neue Schlüssel erstellt wurde, können Sie jederzeit weitere Unterschlüssel für die Signatur oder Verschlüsselung erstellen. Weitere Informationen zu separaten Unterschlüsseln für Signatur und Verschlüsselung finden Sie unter *Mit Unterschlüsseln arbeiten* (auf Seite 75).
- **Schlüsselgröße**: Geben Sie eine Schlüsselgröße zwischen 1024 Bit und 4096 Bit ein. Je größer der Schlüssel, desto sicherer ist er, aber seine Erstellung dauert auch entsprechend länger. Einige Smartcards und Token begrenzen die Schlüsselgröße auf 1024 Bit.

- **Ablaufdatum**: Wählen Sie **Nie** oder geben Sie ein Datum an, an dem das erstellte Schlüsselpaar abläuft.
- **Zulässige Algorithmen**: Deaktivieren Sie alle Algorithmen, die vom erstellten Schlüsselpaar nicht unterstützt werden sollen.
- **Bevorzugter Algorithmus**: Wählen Sie den Algorithmus aus, der in Fällen verwendet werden soll, für die kein Algorithmus festgelegt wurde. Nur ein zulässiger Algorithmus kann als bevorzugter Algorithmus festgelegt werden.
- **Zulässige Hashes**: Deaktivieren Sie die Kontrollkästchen für alle Hashes, die vom erstellten Schlüsselpaar nicht unterstützt werden sollen.
- **Bevorzugter Hash**: Wählen Sie den Hash aus, der verwendet werden soll, wenn kein Hash festgelegt wurde. Nur ein zulässiger Hash kann als bevorzugter Hash festgelegt werden.

10 Klicken Sie auf **OK**, um das Dialogfeld „Erweiterte Schlüsseleinstellungen“ zu schließen.

11 Klicken Sie auf **Weiter**.

12 Wenn Sie in einer von PGP Universal verwalteten Umgebung arbeiten, wird u. U. der Bildschirm „Organisationseinstellungen“ angezeigt. Hier werden die Schlüssel aufgeführt, die der PGP-Administrator zum Hinzufügen zu Ihrer Version von PGP Desktop konfiguriert hat (z. B. der Additional Decryption Key (ADK) des Unternehmens oder der Organisationsschlüssel).

Der Bildschirm „Passphrasenzuweisung“ wird angezeigt.

13 Geben Sie die Passphrase ein, die Sie verwenden möchten, um den exklusiven Zugriff auf den privaten Schlüssel des erstellten Schlüsselpaars beizubehalten.

14 Bestätigen Sie die Eingabe, indem Sie die **Tabulatortaste** drücken, um den Cursor in das Bestätigungsfeld zu setzen. Geben Sie dieselbe Passphrase nochmals ein. Weitere Informationen zur Passphrasen-Qualitätsanzeige finden Sie unter *Passphrasen-Qualitätsanzeige* (siehe "Die Passphrasen-Qualitätsanzeige" auf Seite 352).

Hinweis: Als zusätzliche Sicherheitsmaßnahme werden die für die Passphrase eingegebenen Zeichen in der Regel nicht auf dem Bildschirm angezeigt. Wenn Sie jedoch sicher sind, dass Sie nicht beobachtet werden, und die Zeichen beim Eingeben der Passphrase sehen möchten, aktivieren Sie das Kontrollkästchen **Tastatureingabe anzeigen**.

Warnung: Niemand, auch nicht die PGP Corporation, kann einen Schlüssel wiederherstellen, dessen Passphrase vergessen wurde, es sei denn, der PGP-Administrator hat eine Richtlinie für die PGP-Schlüsselwiederherstellung für Ihr Unternehmen implementiert.

15 Klicken Sie auf **Weiter**, um mit der Schlüsselerstellung zu beginnen. Das neue Schlüsselpaar wird von PGP Desktop erstellt.

Dieser Vorgang kann einige Minuten dauern.

16 Wenn angezeigt wird, dass die Schlüsselerstellung abgeschlossen ist, klicken Sie auf **Weiter**. Sie werden aufgefordert, den öffentlichen Teil des soeben erstellten Schlüssels dem PGP Global Directory hinzuzufügen.

17 Lesen Sie den Text auf dem Bildschirm und klicken Sie auf **Weiter**, um den neuen Schlüssel dem PGP Global Directory hinzuzufügen (empfohlen). Klicken Sie auf **Überspringen**, wenn Sie nicht möchten, dass der öffentliche Schlüssel im PGP Global Directory veröffentlicht wird.

18 Klicken Sie auf **Beenden**. Das neue PGP-Schlüsselpaar wurde erstellt. Es sollte im Arbeitsbereich von PGP Keys angezeigt werden. Falls es nicht aufgeführt ist, stellen Sie sicher, dass im Bedienfeld „PGP Keys“ entweder **Alle Schlüssel** oder **Eigene private Schlüssel** ausgewählt ist.

Achtung: Ziehen Sie zu diesem Zeitpunkt die Erstellung einer Sicherungskopie des privaten Schlüssels an einem sicheren Speicherort in Erwägung. Der private Schlüssel ist sehr wichtig. Sollte er verloren gehen, könnte dies katastrophale Auswirkungen haben, wenn Sie Daten an diesen Schlüssel verschlüsselt haben. Weitere Informationen finden Sie unter *Privaten Schlüssel schützen* (auf Seite 48).

Kennwörter und Passphrasen

Es ist eine schmerzliche Lektion, wenn Sie eine Datei verschlüsseln und dann feststellen, dass sie nicht mehr entschlüsselt werden kann. Jedoch hilft dies, eine Passphrase zu wählen, an die Sie sich erinnern.

Die meisten Anwendungen erfordern ein Kennwort mit einer Länge von drei bis acht Zeichen. Eine Passphrase, die nur aus einem einzigen Wort besteht, ist nicht sicher und von der Verwendung einer solchen Passphrase wird strengstens abgeraten. Ein aus einem einzigen Wort bestehendes Kennwort ist anfällig für Wörterbuchangriffe, bei denen ein Computer alle Wörter eines Wörterbuchs ausprobiert, bis das Kennwort gefunden wurde. Diese Wörterbuchangriffe lassen sich auch ohne großen Aufwand so gestalten, dass eine Vielzahl von Kennwörtern gefunden werden kann, selbst wenn diese leicht von den Wörterbucheinträgen abweichen.

Als Schutz gegen derartige Angriffe wird häufig empfohlen, ein Wort zu erstellen, das eine Kombination aus Groß- und Kleinbuchstaben, Zahlen, Interpunktionszeichen und Leerzeichen enthält. Dies ergibt zwar ein stärkeres Kennwort, jedoch ist es wahrscheinlich auch nicht so leicht zu merken.

Wenn Sie versuchen, einen Wörterbuchangriff durch viele zufällig eingefügte nicht-alphabetische Zeichen zu verhindern, können Sie Ihre Passphrase leicht vergessen. Dies könnte zu einem verheerenden Verlust von Informationen führen, da Sie Ihre eigenen Dateien nicht mehr entschlüsseln können. Eine Passphrase aus mehreren Wörtern ist nicht so anfällig für Wörterbuchangriffe. Falls Sie sich die Passphrase jedoch nicht im Langzeitgedächtnis merken können, haben Sie möglicherweise Schwierigkeiten, sich Wort für Wort daran zu erinnern.

Wenn Sie ein Wort einfach nur spontan auswählen, werden Sie es wahrscheinlich gänzlich vergessen. Sie sollten etwas wählen, das sich bereits in Ihrem Langzeitgedächtnis befindet. Es sollte nichts sein, das Sie in letzter Zeit anderen gegenüber geäußert haben, und auch kein berühmtes Zitat, da die Passphrase für einen geschickten Angreifer nicht einfach zu erraten sein soll. Alles, was bereits tief in Ihrem Langzeitgedächtnis verankert ist, werden Sie wahrscheinlich nicht vergessen. Wenn Sie jedoch leichtsinnig genug sind, die Passphrase aufzuschreiben und den Zettel an Ihren Monitor zu kleben oder in die Schreibtischschublade zu legen, ist es gleichgültig, was Sie wählen.

Weitere Informationen finden Sie unter *Mit Kennwörtern und Passphrasen arbeiten* (auf Seite 351).

Privaten Schlüssel schützen

Die PGP Corporation empfiehlt, dass Sie die folgenden Schritte sofort nach dem Erstellen Ihres Schlüsselpaars ausführen:

Achtung: Wenn Sie diese Schritte nicht ausführen, kann dies in der Zukunft zu einem umfassenden Datenverlust führen.

- Erstellen Sie für den Fall, dass die ursprüngliche Datei des privaten Schlüssels beschädigt wird oder verloren geht, eine Sicherungskopie der Datei an einem anderen, sicheren Speicherplatz. Siehe *Sicherungskopien von privaten Schlüsseln erstellen* (auf Seite 50).
- Denken Sie über die gewählte Passphrase nach, um sicherzustellen, dass Sie sie nicht vergessen. Wenn Sie befürchten, dass Sie während der Erstellung des Schlüssels eine Passphrase festgelegt haben, die Sie möglicherweise wieder vergessen, ändern Sie sie JETZT in eine Passphrase, die Sie nicht vergessen. Informationen zum Ändern der Passphrase finden Sie unter *Passphrase ändern* (auf Seite 68).

Die Datei mit Ihrem privaten Schlüssel ist sehr wichtig, da nach dem Verschlüsseln der Daten an Ihren öffentlichen Schlüssel nur der entsprechende private Schlüssel zum Entschlüsseln der Daten verwendet werden kann. Dies trifft in gleicher Weise auf Ihre Passphrasen zu, denn der Verlust Ihres privaten Schlüssels oder der Passphrase bedeutet, dass Sie Daten, die an einen öffentlichen Schlüssel verschlüsselt wurden, nicht mehr entschlüsseln können. Wenn Sie Daten verschlüsseln, wird hierzu sowohl die Passphrase als auch der private Schlüssel verwendet. Sie benötigen beide, um die verschlüsselten Daten zu entschlüsseln. Nach der Verschlüsselung der Daten kann niemand – nicht einmal die PGP Corporation – die Daten ohne Ihre private Schlüsseldatei und Ihre Passphrase entschlüsseln.

Stellen Sie sich vor, Sie besitzen wichtige verschlüsselte Daten und vergessen dann die Passphrase oder verlieren den privaten Schlüssel. Auf die verschlüsselten Daten kann dann nicht mehr zugegriffen werden, sie können nicht mehr verwendet und auch nicht mehr wiederhergestellt werden.

Schlüssel und Schlüsselbunde schützen

Sie sollten nicht nur Sicherungskopien Ihrer Schlüssel erstellen, sondern auch besonders sorgsam darauf achten, wo Sie den privaten Schlüssel aufbewahren. Obwohl der private Schlüssel durch eine Passphrase geschützt ist, die nur Sie kennen sollten, ist es möglich, dass eine andere Person Ihre Passphrase in Erfahrung bringt und Ihren privaten Schlüssel zum Entschlüsseln von E-Mail-Nachrichten oder zum Fälschen Ihrer digitalen Signatur verwendet. Jemand könnte Ihnen beispielsweise über die Schulter blicken und beobachten, welche Tastatureingaben Sie vornehmen, oder die Tastatureingaben über das Netzwerk oder sogar über das Internet abfangen.

Damit andere Personen, die Ihre Passphrase abgefangen haben, Ihren privaten Schlüssel nicht nutzen können, sollten Sie diesen ausschließlich auf Ihrem eigenen Computer speichern. Falls der Computer mit einem Netzwerk verbunden ist, stellen Sie sicher, dass Ihre Dateien nicht automatisch in eine systemweite Sicherung einbezogen werden, über die andere Personen Zugriff auf Ihren privaten Schlüssel erhalten könnten. Da ein Zugriff auf Computer in einem Netzwerk recht problemlos möglich ist, sollten Sie Ihren privaten Schlüssel auf einer Diskette speichern, falls Sie mit extrem vertraulichen Daten arbeiten. Diese Diskette kann wie ein traditioneller Schlüssel immer dann eingesteckt werden, wenn Sie private Informationen lesen oder signieren möchten.

Als weitere Sicherheitsmaßnahme könnten Sie Ihrer privaten Schlüsselbunddatei einen anderen Namen zuweisen und sie nicht am Standardspeicherort speichern. Geben Sie im Dialogfeld „Optionen“ auf der Registerkarte „Schlüssel“ einen Namen und einen Speicherort für Ihre privaten und öffentlichen Schlüsselbunddateien an.

Ihre privaten und öffentlichen Schlüssel werden in getrennten Schlüsselbunddateien gespeichert. Sie können sie an einen anderen Speicherplatz auf der Festplatte oder auf einer Diskette kopieren. Standardmäßig werden der private Schlüsselbund (`secring.skr`) und der öffentliche Schlüsselbund (`pubring.pkr`) zusammen mit anderen Programmdateien im PGP-Ordner gespeichert. Sicherungskopien können an einem beliebigen Speicherort gespeichert werden.

Für Schlüssel, die auf einer Smartcard erstellt wurden, können keine Sicherungskopien erstellt werden, da der private Teil Ihres Schlüsselpaars nicht exportierbar ist. (Schlüssel können nur unter Windows auf einer Smartcard erstellt werden.)

Sie können PGP Desktop so konfigurieren, dass Schlüsselbunde automatisch nach dem Beenden von >prod< gesichert werden. Legen Sie die Sicherungsoptionen für Schlüsselbunde im Dialogfeld „Optionen“ auf der Registerkarte „Schlüssel“ (Windows) bzw. im Dialogfeld „Einstellungen“ im Bereich „Schlüssel“ (Mac OS X) fest.

Sicherungskopien von privaten Schlüsseln erstellen

So erstellen Sie eine Sicherungskopie Ihres privaten Schlüssels

1. Klicken Sie im Bedienfeld „PGP Keys“ auf **Eigene private Schlüssel**.
2. Wählen Sie das Symbol für Ihr Schlüsselpaar aus.
3. Klicken Sie auf **Datei > Exportieren**.
4. Geben Sie einen Dateinamen ein.
5. Aktivieren Sie das Kontrollkästchen **Private Schlüssel einschließen**. Die ist wichtig, da andernfalls nur Ihr öffentlicher Schlüssel exportiert wird.
6. Klicken Sie auf **Speichern**.
7. Kopieren Sie die Datei (mit der Erweiterung .asc) an einen sicheren Speicherort. Hierbei kann es sich um eine CD handeln, die sorgfältig archiviert wird, um einen anderen PC oder um ein USB-Flash-Laufwerk, das an einem sicheren Ort aufbewahrt wird. Denken Sie daran, dass diese Datei nicht an andere Personen weitergegeben werden darf, da sie sowohl Ihren privaten als auch Ihren öffentlichen Schlüssel enthält.

Hinweis: Wenn Sie in einer von einem PGP Universal Server verwalteten Umgebung arbeiten und den SKM-Schlüsselmodus verwenden, können Sie Ihren Schlüssel nicht mit dieser Methode exportieren. Exportieren Sie Ihr Schlüsselpaar, indem Sie den PGP Universal Server-Administrator bitten, das Schlüsselpaar über die Verwaltungskonsole zu exportieren. Informationen zum Ermitteln des Schlüsselmodus finden Sie unter *Schlüsselmodi* (auf Seite 136).

Vorgehensweise bei verlorenen Schlüsseln

Wenn Sie Ihren Schlüssel verlieren und nicht über eine Sicherungskopie verfügen, von der Sie den Schlüssel wiederherstellen können, können Sie die Informationen, die mit dem Schlüssel verschlüsselt wurden, nie mehr entschlüsseln. Sie können den Schlüssel jedoch wiederherstellen, wenn der PGP-Administrator eine Richtlinie zur Schlüsselwiederherstellung für Ihr Unternehmen implementiert hat. Weitere Informationen finden Sie unter *PGP-Schlüsselwiederherstellung* (siehe "Schlüssel mit PGP Universal Server wiederherstellen" auf Seite 89, "Vorgehensweise bei verloren gegangenen Schlüsseln oder Passphrasen" auf Seite 89). Sie können sich auch an den PGP-Administrator wenden.

Öffentliche Schlüssel verteilen

Nachdem Sie ein PGP Desktop-Schlüsselpaar erstellt haben, müssen Sie den öffentlichen Schlüssel an die Personen übermitteln, mit denen Sie verschlüsselte Nachrichten austauschen möchten.

Sie stellen den öffentlichen Schlüssel anderen Personen bereit, damit diese Ihnen verschlüsselte Informationen senden und Ihre digitale Signatur verifizieren können. Sie benötigen den öffentlichen Schlüssel dieser Personen, um ihnen verschlüsselte Nachrichten senden zu können.

Es gibt verschiedene Möglichkeiten, den öffentlichen Schlüssel zu verteilen:

- *Veröffentlichen Sie den Schlüssel im PGP Global Directory* (siehe "Öffentliche Schlüssel auf einem Keyserver ablegen" auf Seite 51).

  Im Allgemeinen ist keine der anderen Verfahren mehr erforderlich, wenn der Schlüssel in diesem Verzeichnis veröffentlicht wurde.

- *Fügen Sie den öffentlichen Schlüssel in eine E-Mail-Nachricht ein* (siehe "Öffentliche Schlüssel in E-Mail-Nachrichten einfügen" auf Seite 53).

- *Exportieren Sie den öffentlichen Schlüssel oder kopieren Sie ihn in eine Textdatei* (siehe "Öffentliche Schlüssel in Dateien exportieren" auf Seite 53).

Unter Windows ist auch Folgendes möglich:

- *Kopieren Sie die Informationen von einer Smartcard direkt auf den Schlüsselbund einer anderen Person* (siehe "Direkt von einer Smartcard auf den Schlüsselbund einer anderen Person kopieren" auf Seite 54).

Öffentliche Schlüssel auf einem Keyserver ablegen

Die beste Methode zur Bereitstellung eines öffentlichen Schlüssels an andere besteht darin, ihn auf einem öffentlichen Keyserver (einer großen Datenbank mit Schlüsseln) abzulegen, damit alle darauf zugreifen können. Auf diese Weise können Ihnen andere Personen verschlüsselte E-Mail-Nachrichten senden, ohne ausdrücklich eine Kopie Ihres Schlüssels anfordern zu müssen. Gleichzeitig müssen weder Sie noch andere Personen eine große Anzahl öffentlicher Schlüssel speichern, die Sie selten verwenden.

Weltweit gibt es zahlreiche Keyserver (darunter das PGP Global Directory), auf denen Sie Ihren Schlüssel allgemein zugänglich machen können. Falls Sie PGP Desktop in einer Domäne einsetzen, die durch einen PGP Universal Server geschützt ist, hat der PGP-Administrator PGP Desktop mit entsprechenden Einstellungen vorkonfiguriert.

Wenn Sie einen öffentlichen Keyserver nutzen, beachten Sie beim Senden des Schlüssels Folgendes:

- Ist dies tatsächlich der Schlüssel, den Sie verwenden möchten? Andere Personen, die mit Ihnen kommunizieren möchten, könnten wichtige Informationen an diesen Schlüssel verschlüsseln. Aus diesem Grund sollten Sie nur Schlüssel auf einem Keyserver platzieren, die tatsächlich von anderen verwendet werden sollen.
- Können Sie sich an die Passphrase für diesen Schlüssel erinnern, damit Sie Daten abrufen können, die an den Schlüssel verschlüsselt wurden, oder damit Sie den Schlüssel widerrufen können, falls Sie ihn nicht mehr verwenden möchten?
- Anders als beim PGP Global Directory bleibt ein einmal hochgeladener Schlüssel auf dem Server. Einige öffentliche Keyserver lassen das Löschen von Schlüsseln nicht zu. Andere Server wiederum bieten Replizierungsfunktionen, die Schlüssel auch auf andere Keyserver kopieren. Selbst wenn Sie einen Schlüssel von einem Server löschen, könnte er später wieder auf einem anderen Server auftauchen.

Die meisten Benutzer legen den öffentlichen Schlüssel unmittelbar nach dem Erstellen des Schlüsselpaars im PGP Global Directory ab. Wenn Sie den Schlüssel bereits im PGP Global Directory abgelegt haben, müssen Sie diesen Vorgang nicht wiederholen. In den meisten Fällen ist es nicht notwendig, den Schlüssel auf einem anderen Keyserver zu veröffentlichen. Beachten Sie auch, dass Schlüssel auf anderen Keyservern u. U. nicht verifiziert werden, sodass möglicherweise ein höherer Zeitaufwand Ihrerseits erforderlich ist, um sich mit dem Besitzer des Keyservers in Kontakt zu setzen und den Fingerabdruck zu verifizieren.

So senden Sie Ihren öffentlichen Schlüssel manuell an einen Keyserver

1. Öffnen Sie PGP Desktop.
2. Achten Sie darauf, dass das Bedienfeld „PGP Keys“ ausgewählt ist.
3. Klicken Sie mit der rechten Maustaste auf das Schlüsselpaar, dessen öffentlichen Schlüssel Sie zum Keyserver senden möchten.
4. Klicken Sie auf **Senden an**. Wählen Sie in der Liste den Keyserver aus, an den Sie den öffentlichen Schlüssel senden wollen. Falls der Keyserver, an den Sie den öffentlichen Schlüssel senden möchten, nicht in der Liste aufgeführt wird, finden Sie weitere Informationen unter *Mit Keyservern arbeiten* (auf Seite 56). PGP Desktop informiert Sie, wenn der öffentliche Schlüssel erfolgreich auf den Keyserver kopiert wurde.

Sobald Sie eine Kopie Ihres öffentlichen Schlüssels auf einem Keyserver platziert haben, ist er für andere Personen verfügbar, die Ihnen verschlüsselte Daten senden oder Ihre digitale Signatur verifizieren möchten. Auch wenn Sie andere Benutzer nicht ausdrücklich auf Ihren öffentlichen Schlüssel hinweisen, können diese eine Kopie davon abrufen, indem sie den Keyserver nach Ihrem Namen oder Ihrer E-Mail-Adresse durchsuchen.

Viele Benutzer geben die Webadresse für ihren öffentlichen Schlüssel am Ende ihrer E-Mail-Nachrichten an. In den meisten Fällen kann der Empfänger einfach auf die Adresse doppelklicken, um auf eine Kopie Ihres Schlüssels auf dem Server zuzugreifen. Einige Benutzer drucken ihren PGP-Fingerabdruck sogar auf ihre Visitenkarte, um die Verifizierung zu erleichtern.

Öffentliche Schlüssel in E-Mail-Nachrichten einfügen

Eine weitere praktische Methode zur Übermittlung des öffentlichen Schlüssels an andere ist das Einfügen des Schlüssels in eine E-Mail-Nachricht.

Wenn Sie einer anderen Person Ihren öffentlichen Schlüssel senden, achten Sie darauf, die E-Mail-Nachricht zu signieren. Auf diese Weise kann der Empfänger Ihre Signatur verifizieren und sicherstellen, dass niemand die Daten bei der Übermittlung verfälscht hat. Falls Ihr Schlüssel jedoch noch nicht von einer Vertrauensperson signiert wurde, können die Empfänger Ihrer Signatur nur dann sicher sein, dass die Signatur von Ihnen stammt, wenn Sie den Fingerabdruck auf Ihrem Schlüssel verifizieren.

So hängen Sie Ihren öffentlichen Schlüssel an eine E-Mail-Nachricht an

1. Stellen Sie in PGP Desktop sicher, dass das Bedienfeld „PGP Keys“ ausgewählt ist.
2. Klicken Sie mit der rechten Maustaste auf das Schlüsselpaar, dessen öffentlichen Schlüssel Sie an eine E-Mail-Nachricht anhängen möchten.
3. Klicken Sie auf **Senden an** und wählen Sie **E-Mail-Empfänger** aus. Die E-Mail-Anwendung wird geöffnet, wobei die Schlüsselinformationen bereits eingefügt wurden.
4. Adressieren Sie die Nachricht und senden Sie sie.

Wenn dieses Verfahren in Ihrem Fall nicht funktioniert, können Sie alternativ PGP Desktop öffnen, Ihr Schlüsselpaar auswählen und auf **Bearbeiten > Kopieren** klicken. Öffnen Sie eine E-Mail-Nachricht und fügen Sie den öffentlichen Schlüssel in den Nachrichtentext ein. Bei einigen E-Mail-Anwendungen können Sie den Schlüssel einfach aus PGP Desktop in den Text der E-Mail-Nachricht ziehen, um die Daten des öffentlichen Schlüssels zu übertragen.

Öffentliche Schlüssel in Dateien exportieren

Eine andere Methode zum Verteilen des öffentlichen Schlüssels besteht darin, ihn in eine Datei zu exportieren. Diese Datei stellen Sie dann der Person zur Verfügung, mit der Sie sicher kommunizieren möchten.

Es gibt drei Möglichkeiten, den öffentlichen Schlüssel in eine Datei zu exportieren oder ihn in einer Datei zu speichern:

- Wählen Sie das Schlüsselpaar aus und klicken Sie auf **Datei > Exportieren**. Geben Sie einen Namen und einen Speicherort für die Datei an und klicken Sie auf **Speichern**. Achten Sie darauf, den privaten Schlüssel *keinesfalls* zusammen mit dem öffentlichen Schlüssel zu speichern, wenn Sie diese Datei an andere Personen weitergeben möchten.
- Klicken Sie bei gedrückter Ctrl-Taste auf den Schlüssel, den Sie in einer Datei speichern möchten. Wählen Sie **Exportieren**, geben Sie einen Namen und einen Speicherort für die Datei ein und klicken Sie auf **Speichern**. Achten Sie darauf, den privaten Schlüssel *keinesfalls* zusammen mit dem öffentlichen Schlüssel zu speichern, wenn Sie diese Datei an andere Personen weitergeben möchten.
- Wählen Sie das Schlüsselpaar aus und klicken Sie auf **Bearbeiten > Kopieren**. Öffnen Sie ein Textbearbeitungsprogramm und wählen Sie **Einfügen** aus, um die Schlüsselinformationen in die Textdatei einzufügen. Speichern Sie dann die Datei. Sie können die Datei danach per E-Mail versenden oder an andere Personen weitergeben. Der Empfänger muss auf seinem System PGP Desktop verwenden, um den öffentlichen Teil des Schlüssels abrufen zu können.

Direkt von einer Smartcard auf den Schlüsselbund einer anderen Person kopieren

Wenn sich Ihr öffentlicher Schlüssel auf einer Smartcard befindet, können Sie ihn von dort direkt auf den Schlüsselbund einer anderen Person kopieren und ihn auf diese Weise verteilen.

Weitere Informationen dazu finden Sie unter *Öffentliche Schlüssel von Smartcards auf Schlüsselbunde kopieren* (auf Seite 318).

Öffentliche Schlüssel anderer Personen erhalten

Ebenso, wie Sie Ihren öffentlichen Schlüssel an alle Personen weitergeben müssen, die Ihnen verschlüsselte E-Mail-Nachrichten senden oder Ihre digitale Signatur verifizieren möchten, benötigen Sie die öffentlichen Schlüssel anderer Personen, denen Sie verschlüsselte E-Mail-Nachrichten senden oder deren digitale Signatur Sie verifizieren möchten.

Es gibt verschiedene Möglichkeiten, den öffentlichen Schlüssel einer anderen Person zu erhalten:

- Automatisches Abrufen des verifizierten Schlüssels aus dem PGP Global Directory
- Manuelles Suchen des Schlüssels auf einem öffentlichen Keyserver

- Automatisches Hinzufügen des öffentlichen Schlüssels aus einer E-Mail-Nachricht an den eigenen Schlüsselbund
- Importieren des öffentlichen Schlüssels aus einer exportierten Datei
- Abrufen des Schlüssels vom PGP Universal Server Ihrer Organisation

Öffentliche Schlüssel sind lediglich Textblöcke. Sie können dem Schlüsselbund problemlos hinzugefügt werden, indem sie aus einer Datei importiert oder aus einer E-Mail-Nachricht kopiert und in den öffentlichen Schlüsselbund in PGP Desktop einfügt werden.

Öffentliche Schlüssel von einem Keyserver abrufen

Wenn der Empfänger der verschlüsselten E-Mail-Nachricht ein erfahrener PGP Desktop-Benutzer ist, befindet sich wahrscheinlich eine Kopie seines öffentlichen Schlüssels im PGP Global Directory oder auf einem anderen öffentlichen Keyserver. Somit können Sie jederzeit eine Kopie seines aktuellen Schlüssels abrufen, wenn Sie eine E-Mail-Nachricht an diesen Empfänger senden möchten, und müssen auf Ihrem öffentlichen Schlüsselbund keine unüberschaubare Zahl von Schlüsseln speichern.

Es gibt eine Vielzahl von öffentlichen Keyservern, z. B. das von der PGP Corporation gehostete PGP Global Directory, auf denen die Schlüssel der meisten PGP-Benutzer zu finden sind. Wenn Ihnen der Empfänger keine Internet-Adresse mitgeteilt hat, unter der sein öffentlicher Schlüssel gespeichert ist, können Sie auf einen beliebigen Keyserver zugreifen und nach dem Namen oder der E-Mail-Adresse des Benutzers suchen. Die Suche führt nicht in jedem Fall zum Erfolg, da nicht alle öffentlichen Keyserver regelmäßig mit dem Schlüsseldatenbestand der anderen Server synchronisiert werden.

Falls Sie in einer Domäne arbeiten, die durch einen PGP Universal Server geschützt ist, kann der PGP-Administrator ggf. vorgeben, dass der in den PGP Universal Server integrierte Keyserver verwendet werden muss. In diesem Fall ist PGP Desktop wahrscheinlich bereits für den Zugriff auf den entsprechenden PGP Universal Server konfiguriert.

Der PGP Universal Server ist seinerseits standardmäßig für die Kommunikation mit dem PGP Global Directory konfiguriert. Dadurch werden Schlüsselsuche und -verifizierung auf verschiedene PGP-Anwendungen verteilt.

So rufen Sie den öffentlichen Schlüssel einer anderen Person von einem Keyserver ab

1. Öffnen Sie PGP Desktop und markieren Sie auf das Bedienfeld PGP-Schlüssel.
2. Wählen Sie im Bedienfeld PGP-Schlüssel die Option **Nach Schlüsseln suchen**. Im Arbeitsbereich wird der Bildschirm „Nach Schlüsseln suchen“ angezeigt.

3 Legen Sie die Suchkriterien fest und klicken Sie auf **Suchen**. Wenn Sie nur einen bestimmten Keyserver durchsuchen möchten, klicken Sie in das Feld **Suchen** und wählen den Keyserver. Wenn der Keyserver, auf dem Sie suchen möchten, derzeit nicht in der Liste ist, klicken Sie auf **Keyserver-Liste bearbeiten** und fügen Sie ihn hinzu.

   Bei der Suche nach Schlüsseln auf einem Keyserver können Sie Angaben für verschiedene Schlüsselmerkmale festlegen. Für die meisten Operationen steht auch die Umkehrung zur Verfügung. So können Sie beispielsweise eine Suche mit dem Kriterium „Benutzer-ID ist nicht Peter“ durchführen.

   Die Ergebnisse der Suche werden angezeigt.

4 Wenn bei der Suche ein öffentlicher Schlüssel gefunden wurde, den Sie zu Ihrem Schlüsselbund hinzufügen möchten, klicken Sie im Bedienfeld PGP-Schlüssel auf **Zu eigenem Schlüsselbund hinzufügen**. Der ausgewählte Schlüssel wird dem Schlüsselbund hinzugefügt.

Tipp: Wenn Sie mithilfe der Suchkriterien nach einem sehr gängigen Namen suchen (z. B. „Name enthält Stefan“), wird nur die erste Übereinstimmung zurückgegeben. Dieses Verhalten ist beabsichtigt, um das nicht autorisierte, massenhafte Abfragen von Schlüsseln (das so genannte Harvesting) zum Zweck des Phishing zu verhindern. Wenn Sie gängige Namen oder Domänen verwenden, müssen Sie möglicherweise den vollständigen Namen oder die gesamte E-Mail-Adresse eingeben, um den richtigen Schlüssel zu finden.

Öffentliche Schlüssel aus E-Mail-Nachrichten übernehmen

Eine praktische Methode zum Übermitteln eines öffentlichen Schlüssels besteht darin, den Schlüssel als Anlage einer E-Mail-Nachricht zu senden.

So fügen Sie einen öffentlichen Schlüssel hinzu, den Sie als Anlage einer E-Mail-Nachricht erhalten

1 Öffnen Sie die E-Mail-Nachricht.

2 Doppelklicken Sie auf die ASC-Datei, die den öffentlichen Schlüssel enthält. PGP Desktop erkennt das Dateiformat und öffnet das Dialogfeld „Schlüssel auswählen“.

3 Bestätigen Sie die Abfrage zum Öffnen der Datei.

4 Wählen Sie die öffentlichen Schlüssel aus, die Sie Ihrem Schlüsselbund hinzufügen möchten, und klicken Sie auf **Importieren**.

Mit Keyservern arbeiten

PGP Desktop erkennt folgende Arten von Keyservern:

- **PGP Universal-Keyserver**: Wenn Sie PGP Desktop in einer Domäne einsetzen, die durch einen PGP Universal Server geschützt ist, ist PGP Desktop für die ausschließliche Kommunikation mit dem Keyserver vorkonfiguriert, der in den entsprechenden PGP Universal Server integriert ist. Für PGP Desktop handelt es sich hierbei um einen vertrauenswürdigen Keyserver. PGP Desktop vertraut daher automatisch allen Schlüsseln auf diesem Keyserver, sofern der PGP Universal Server nicht signalisiert, dass der betreffende Schlüssel nicht vertrauenswürdig ist. Dies kann beispielsweise bei der Verifizierung der Signaturen von Remoteschlüsseln der Fall sein.

  Die Adresse eines PGP Universal-Keyservers kann z. B. folgendermaßen lauten: https://keyserver.beispiel.com.

- **PGP Global Directory**: Wenn Sie PGP Desktop außerhalb einer Domäne einsetzen, die durch einen PGP Universal Server geschützt ist, ist PGP Desktop für die Kommunikation mit dem *PGP Global Directory* (https://keyserver.pgp.com) vorkonfiguriert.

  Das PGP Global Directory ist ein kostenloser, frei zugänglicher Keyserver, der von der PGP Corporation gehostet wird und schnellen und einfachen Zugriff auf PGP-Schlüssel ermöglicht. Es nutzt eine Keyserver-Technologie der nächsten Generation. Mit dieser Technologie werden die Schlüssel verifiziert, die einer E-Mail-Adresse zugeordnet sind, sodass der Keyserver nicht durch unbenutzte oder gefälschte Schlüssel, durch mehrere Schlüssel pro E-Mail-Adresse und andere Probleme belastet wird, die bei älteren Keyservern anzutreffen waren. Außerdem können Sie Ihre eigenen Schlüssel verwalten und u. a. Ihre eigenen Schlüssel ersetzen und löschen sowie Schlüsseln weitere E-Mail-Adressen hinzufügen Durch die Verwendung des PGP Global Directory haben Sie wesentlich bessere Chancen, den öffentlichen Schlüssel einer Person zu finden, der Sie sichere Nachrichten senden möchten.

  Das PGP Global Directory wird von PGP Desktop als vertrauenswürdiger Keyserver angesehen. PGP Desktop vertraut daher automatisch allen Schlüsseln, die dort gefunden werden. Während des anfänglichen Verbindungsaufbaus mit dem PGP Global Directory wird der PGP Global Directory-Überprüfungsschlüssel heruntergeladen, signiert und von dem Schlüssel als vertrauenswürdig eingestuft, den Sie im PGP Global Directory veröffentlichen. Der PGP Global Directory-Schlüssel wird darüber hinaus Ihrem Schlüsselbund hinzugefügt. Somit werden alle vom PGP Global Directory verifizierten Schlüssel von PGP Desktop als gültig betrachtet.

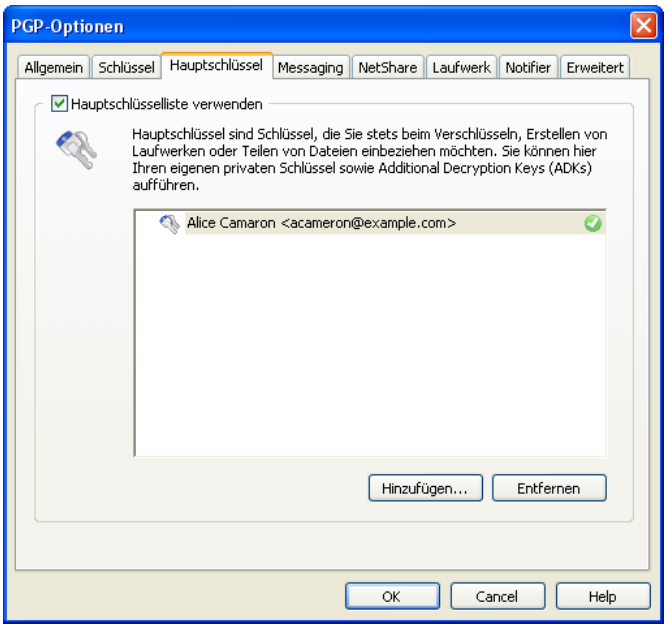
  PGP Universal-Dienstprotokoll: Das PGP Universal-Dienstprotokoll (USP) ist ein SOAP-Protokoll, das über HTTP/HTTPS-Standardports ausgeführt wird. Dies ist der Standardmechanismus für die Schlüsselsuche. Wenn Sie in einer von einem PGP Universal Server verwalteten Umgebung arbeiten, wird PGP USP für alle Anforderungen für die Schlüsselsuche sowie für die gesamte Kommunikation zwischen dem PGP Universal Server und PGP Desktop verwendet.

- **Andere Keyserver**: In den meisten Fällen handelt es sich hierbei um andere öffentliche Keyserver. Unter Umständen können Sie jedoch z. B. über Ihr Unternehmen auf einen privaten Keyserver zugreifen.

Weitere Informationen zum Arbeiten mit Keyservern finden Sie unter *Schlüsseloptionen* (auf Seite 330).

Hauptschlüssel verwenden

Die Hauptschlüsselliste enthält eine Reihe von Schlüsseln, die Sie standardmäßig jedes Mal hinzufügen möchten, wenn Sie Schlüssel für Messaging, Laufwerksverschlüsselung, PGP NetShare oder PGP Zip auswählen. Die betreffenden Schlüssel müssen in diesem Fall nicht mehr in das Feld **Empfänger** gezogen werden.



Hinweis: Wenn Sie Ihren Schlüssel mithilfe des Einrichtungsassistenten erstellt haben, wird er der Hauptschlüsselliste automatisch hinzugefügt. Wenn Sie die Schlüsselerstellung übersprungen und den Schlüssel in PGP Desktop importiert haben, wird der Schlüssel nicht automatisch der Liste hinzugefügt.

Der Hauptschlüsselliste Schlüssel hinzufügen

▸ **So fügen Sie der Hauptschlüsselliste Schlüssel hinzu**

1 Klicken Sie in PGP Desktop auf **Extras > Optionen**.

2 Wählen Sie die Registerkarte „Hauptschlüssel“ aus.

3 Wenn Sie die Hauptschlüsselliste verwenden möchten, aktivieren Sie das Kontrollkästchen **Hauptschlüssellisteverwenden. Sie können nur Schlüssel in die Hauptschlüsselliste aufnehmen bzw. daraus entfernen, wenn dieses Kontrollkästchen aktiviert ist.**

4 Klicken Sie auf **Hinzufügen**. Das Dialogfeld „Hauptschlüssel auswählen“ wird angezeigt.

5 Wählen Sie in der Liste **Schlüsselquelle** auf der linken Seite die Schlüssel aus, die Sie verwenden möchten. Halten Sie beim Klicken die Umschalt- bzw. die Strg-Taste gedrückt, um mehrere Schlüssel auszuwählen.

6 Wählen Sie die gewünschten Schlüssel aus und klicken Sie auf **Hinzufügen**.

Tipp: Wenn die Liste **Hinzuzufügende Schlüssel auf der rechten Seite Schlüssel enthält, die Sie nicht benötigen, wählen Sie diese Schlüssel aus und klicken Sie auf Entfernen**.

7 Klicken Sie nach Auswahl der Schlüssel auf **OK.** Die ausgewählten Schlüssel werden in der Hauptschlüsselliste angezeigt.

Schlüssel aus der Hauptschlüsselliste löschen

▸ **So entfernen Sie Schlüssel aus der Hauptschlüsselliste**

1 Klicken Sie in PGP Desktop auf **Extras > Optionen**.

2 Wählen Sie die Registerkarte „Hauptschlüssel“ aus.

3 Wenn Sie die Hauptschlüsselliste verwenden möchten, aktivieren Sie das Kontrollkästchen **Hauptschlüssellisteverwenden. Sie können nur Schlüssel in die Hauptschlüsselliste aufnehmen bzw. daraus entfernen, wenn dieses Kontrollkästchen aktiviert ist.**

4 Wählen Sie die Schlüssel aus, die Sie entfernen möchten. Halten Sie beim Klicken die Umschalt- bzw. die Strg-Taste gedrückt, um mehrere Schlüssel auszuwählen.

5 Klicken Sie auf **Entfernen.** Die Schlüssel werden entfernt.

6 PGP-Schlüssel verwalten

In diesem Abschnitt wird beschrieben, wie Sie Schlüssel mit PGP Desktop verwalten.

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung verwenden, hat Ihr PGP Universal Server-Administrator ggf. bestimmte Funktionen deaktiviert. Ist eine Funktion deaktiviert, wird das Bedienelement auf der linken Seite nicht angezeigt und das Menü oder andere auf diese Funktion zutreffenden Optionen sind nicht verfügbar. Die in diesem Handbuch enthaltenen Abbildungen entsprechen der Standardinstallation, bei der alle Funktionen aktiviert sind. Wenn Ihr PGP Universal Server-Administrator diese Funktion deaktiviert hat, ist dieser Abschnitt für Sie nicht relevant.

In diesem Kapitel

Schlüsseleigenschaften anzeigen und festlegen 62
Mit Foto-IDs arbeiten 63
Benutzernamen und E-Mail-Adressen in einem Schlüssel verwalten 64
Schlüssel und X.509-Zertifikate importieren 65
Passphrase ändern 68
Schlüssel, Benutzer-IDs und Signaturen löschen 69
Öffentliche Schlüssel deaktivieren und aktivieren 70
Einen öffentlichen Schlüssel verifizieren 71
Öffentliche Schlüssel signieren 72
Vertrauen für Schlüsselvalidierungen gewähren 74
Mit Unterschlüsseln arbeiten 75
Mit ADKs arbeiten 81
Mit Widerrufern arbeiten 83
Schlüssel teilen und wieder zusammenfügen 85
Vorgehensweise bei verloren gegangenen Schlüsseln oder Passphrasen 89
Schlüssel schützen 94

Schlüsseleigenschaften anzeigen und festlegen

Im Arbeitsbereich von PGP Keys können die folgenden wichtigen Details zu Ihren Schlüsseln angezeigt werden:

- Name
- E-Mail-Adresse
- Gültigkeit
- Größe
- Schlüssel-ID
- Vertrauen
- Erstellungsdatum
- Ablaufdatum
- ADK
- Status
- Schlüsselbeschreibung
- Schlüsselverwendung

Sie können einstellen, welche Details angezeigt werden sollen, indem Sie auf **Schlüssel** klicken und die angezeigten Spalten über **Ansicht > Spalten** festlegen.

Sie erhalten jedoch mehr Informationen zu einem Schlüssel, wenn Sie die Schlüsseleigenschaften anzeigen. Einige der hier aufgeführten Informationen können auch geändert werden.

Hinweis: Wenn Sie in einer von einem PGP Universal Server verwalteten Umgebung arbeiten und den SKM-Schlüsselmodus verwenden, können Sie keine Änderungen an Ihrem Schlüssel vornehmen. Zudem laufen SKM-Schlüssel grundsätzlich nicht ab. Informationen zum Ermitteln des Schlüsselmodus finden Sie unter *Schlüsselmodi* (auf Seite 136).

So zeigen Sie die Eigenschaften eines Schlüssels an

1. Öffnen Sie PGP Desktop, klicken Sie auf das Bedienfeld „PGP-Schlüssel“ und klicken Sie im Bedienfeld auf **Alle Schlüssel**. Alle Schlüssel am Schlüsselbund werden angezeigt.

2 Doppelklicken Sie auf den Schlüssel, dessen Eigenschaften Sie anzeigen möchten. Das Dialogfeld „Schlüsseleigenschaften“ für den von Ihnen ausgewählten Schlüssel wird angezeigt.

Mit Foto-IDs arbeiten

Sie können Ihren Diffie-Hellman/DSS- und RSA-Schlüsseln eine Foto-ID hinzufügen.

So fügen Sie dem Schlüssel ein Foto hinzu

1 Öffnen Sie PGP Desktop, klicken Sie auf das Bedienfeld „PGP-Schlüssel“ und wählen Sie **Eigene privaten Schlüssel** aus.

2 Doppelklicken Sie im Arbeitsbereich „PGP Keys“ auf den privaten Schlüssel, dem Sie die Foto-ID hinzufügen möchten. Das Dialogfeld „Schlüsseleigenschaften“ für den ausgewählten Schlüssel wird angezeigt.

3 Klicken Sie mit der rechten Maustaste auf das Platzhaltersymbol und wählen Sie **Foto-ID hinzufügen** aus. Das Dialogfeld „Foto hinzufügen“ wird angezeigt.

4 Ziehen Sie das Foto ins Dialogfeld „Foto hinzufügen“, kopieren Sie es hinein oder klicken Sie auf **Datei auswählen**, um nach dem Foto zu suchen.

5 Klicken Sie auf **OK**. Das Passphrasen-Dialogfeld wird geöffnet.

6 Geben Sie die Passphrase für den Schlüssel ein, den Sie ändern möchten, und klicken Sie auf **OK**. Die Foto-ID wird dem öffentlichen Schlüssel hinzugefügt.

So löschen Sie eine Foto-ID

- Klicken Sie mit der rechten Maustaste im Dialogfeld „Schlüsseleigenschaften“ auf das Foto und wählen Sie **Foto-ID entfernen** aus. Das Foto wird vom Schlüssel entfernt.

So kopieren Sie eine Foto-ID

- Klicken Sie mit der rechten Maustaste im Dialogfeld „Schlüsseleigenschaften“ auf das Foto und wählen Sie **Foto-ID kopieren** aus. Dann können Sie das Foto in einen anderen Schlüssel oder in ein Grafikprogramm einfügen.

Benutzernamen und E-Mail-Adressen in einem Schlüssel verwalten

PGP Desktop unterstützt mehrere Benutzernamen und E-Mail-Adressen auf einem Schlüsselpaar. Anhand dieser Namen und E-Mail-Adressen können andere Personen Ihren Schlüssel ermitteln, um Ihnen verschlüsselte Nachrichten zu senden.

So fügen Sie dem Schlüssel einen neuen Benutzernamen oder eine neue E-Mail-Adresse hinzu

1. Öffnen Sie PGP Desktop, klicken Sie auf das Bedienfeld „PGP-Schlüssel“ und wählen Sie **Eigene privaten Schlüssel** aus.
2. Doppelklicken Sie im Arbeitsbereich von PGP Keys auf den privaten Schlüssel, dem Sie einen Benutzernamen oder eine E-Mail-Adresse hinzufügen möchten. Das Dialogfeld „Schlüsseleigenschaften“ wird für den Schlüssel angezeigt, auf den Sie doppelgeklickt haben.
3. Klicken Sie auf **E-Mail-Adresse hinzufügen**. Das Dialogfeld Neuer „PGP-Benutzername“ wird angezeigt.
4. Geben Sie den Namen und die E-Mail-Adresse in die vorgesehenen Felder ein und klicken Sie auf **OK**. Das Dialogfeld „PGP-Passphrase für Schlüssel eingeben“ wird angezeigt.
5. Geben Sie die Passphrase für den privaten Teil des Schlüssels ein, den Sie ändern, und klicken Sie auf **OK**.
6. Wenn Sie den neuen Benutzernamen und die neue E-Mail-Adresse als primären Bezeichner für den Schlüssel festlegen möchten, klicken Sie im Dialogfeld „Schlüsseleigenschaften“ auf den Namen des aktuellen primären Bezeichners und wählen Sie den Benutzer aus, den Sie gerade hinzufügt haben.

7 Schließen Sie das Dialogfeld „Schlüsseleigenschaften“. Der neue Name wird in der Liste der Schlüssel in PGP Desktop am Ende der Liste der Benutzernamen eingefügt, die diesem Schlüssel zugewiesen wurden.

So ändern Sie den primären Bezeichner, der mit Ihrem Schlüssel assoziiert ist

1 Führen Sie einen der folgenden Schritte aus:

- Klicken Sie im Dialogfeld „Schlüsseleigenschaften“ auf den Namen des aktuellen primären Schlüsseleigentümers und wählen Sie den Namen des Benutzers aus der angezeigten Liste aus.
- Erweitern Sie in PGP Desktop Ihren Schlüssel in der Schlüsselliste, klicken Sie mit der rechten Maustaste auf den Benutzernamen, den Sie als primären Namen festlegen möchten, und klicken Sie im Kontextmenü auf **Als primären Namen festlegen**.

So löschen Sie einen Namen oder eine E-Mail-Adresse aus dem Schlüsselpaar

1 Klicken Sie in der Schlüsselliste auf das Pluszeichen links neben dem Schlüssel, um den Schlüssel zu erweitern.

2 Wählen Sie die Benutzer-ID aus, die Sie löschen möchten.

3 Drücken Sie die Entfernen-Taste auf der Tastatur. Ein Bestätigungsdialogfeld wird angezeigt.

Tipp: Sie können auch auf **Bearbeiten > Löschen** (Windows) oder auf **Bearbeiten > Entfernen** (Mac OS X) klicken.

4 Klicken Sie auf **Löschen**. Die Benutzer-ID wird gelöscht.

Schlüssel und X.509-Zertifikate importieren

Sie können öffentliche PGP-Schlüssel und Zertifikate vom Typ PKCS-12 X.509 (ein digitales Zertifikat, das von den meisten Webbrowsern verwendet wird) sowie öffentliche Zertifikate vom Typ PKCS-7 X.509 in Ihren PGP Desktop-Schlüsselbund importieren. Sie können auch X.509-Zertifikate im PEM-Format (Privacy Enhanced Mail) von Ihrem Browser importieren, indem Sie sie in Ihren öffentlichen Schlüsselbund kopieren.

Es gibt mehrere Methoden, den öffentlichen PGP-Schlüssel eines anderen Benutzers zu importieren und dem Schlüsselbund hinzuzufügen. Dies umfasst folgende Möglichkeiten:

- Doppelklicken Sie auf die Datei in Ihrem System. Falls PGP Desktop das Dateiformat erkennt, wird die Datei geöffnet und Sie werden aufgefordert, den Import der Schlüssel in der Datei zu bestätigen.
- Wählen Sie in PGP Desktop die Schlüsseldatei für den Import aus.
- Ziehen Sie die Datei mit dem öffentlichen Schlüssel in das Fenster von PGP Keys.

PGP Desktop verfügt über einen Assistenten für den Zertifikatimport, um diese Aufgabe zu vereinfachen. Weitere Informationen finden Sie unter *Den Assistenten für den Zertifikatimport verwenden* (auf Seite 66).

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen und während der Anmeldung ein X.509-Zertifikat auf einem Token importiert haben (d. h. Sie haben die Option zum Importieren des Zertifikats als PGP-Schlüssel ausgewählt), müssen Sie die Option **Schlüsselbund mit Token und Smartcards synchronisieren** manuell aktivieren. Klicken Sie dazu in PGP Desktop auf **Extras > Optionen** und wählen Sie die Registerkarte „Schlüssel“ aus. Dieser Schritt ist erforderlich, damit die Schlüssel ordnungsgemäß mit PGP Whole Disk Encryption funktionieren.

Den Assistenten für den Zertifikatimport verwenden

X.509-Zertifikate können aus Dateien, dem persönlichen Zertifikatsspeicher von Windows oder von Smartcards in PGP Desktop importiert werden. Sogar Smartcard-basierte Zertifikate, die im Zertifikatsspeicher von Windows angezeigt werden, können importiert werden. Der Assistent für den Zertifikatimport unterstützt Sie beim Importvorgang.

Wenn Zertifikate aus Dateien importiert werden, kann das Zertifikat nur aus einer Datei mit der Erweiterung PEM, PFX, P7b oder P12 importiert werden.

Hinweise: Werden Zertifikate aus dem persönlichen Zertifikatsspeicher von Windows verwendet, werden Sie möglicherweise von Windows (oder der Smartcard-Software eines Drittanbieters, falls Smartcard-basierte persönliche Windows-Zertifikate verwendet werden) aufgefordert, das Kennwort des Zertifikats bzw. die PIN einzugeben.

Einige Vorgänge, z. B. das Ändern des Kennworts des Zertifikats, können nicht über PGP Desktop ausgeführt werden, wenn Zertifikate aus dem persönlichen Zertifikatsspeicher von Windows verwendet werden. Verwenden Sie die Software von Windows (oder der Smartcard), um solche Vorgänge auszuführen.

So importieren Sie ein Zertifikat mit dem Assistenten für den Zertifikatimport

Vor dem Import: Vergewissern Sie sich, dass Ihnen die Passphrase für das zu importierende Zertifikat bekannt ist.

1. Starten Sie den Assistenten. Dafür haben Sie folgende Möglichkeiten:
   - Klicken Sie auf **Datei > Öffnen**.
   - Klicken Sie auf **Datei > Persönliche Zertifikate importieren**.
   - Ziehen Sie die Datei mit dem öffentlichen Schlüssel in das Fenster von PGP Keys.
2. Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen und der Administrator definiert hat, dass Sie die Methode für den Zertifikatimport auswählen können, wählen Sie Folgendes aus:
   - **Auf einen vorhandenen Schlüssel**: Das Zertifikat wird einem Schlüssel hinzugefügt, der sich bereits an Ihrem Schlüsselbund befindet.
   - **Als neue PGP-Schlüssel**: Mithilfe des importierten Zertifikats wird ein neuer PGP-Schlüssel erstellt.
   - **Als PGP X.509-Wrapper-Schlüssel**: Mithilfe des importierten Zertifikats wird ein neuer PGP-Schlüssel erstellt. PGP Desktop behandelt den neuen Schlüssel als X.509-Zertifikat.
3. Wählen Sie die gewünschte Option aus und klicken Sie auf **Weiter**. Es wird entweder der Bildschirm „Eingabe der Zertifikat-Passphrase“ oder das Dialogfeld „PGP-Passphrase eingeben“ angezeigt.
4. Geben Sie das Kennwort für das Zertifikat ein und klicken Sie auf **Weiter**.
   - Wenn Sie ein Zertifikat mit der Option **Auf einen vorhandenen Schlüssel** importieren, wird der Bildschirm **Schlüssel auswählen** angezeigt. Fahren Sie mit dem nächsten Schritt fort.
   - Wenn Sie das Zertifikat mit der Option **Als neue PGP-Schlüssel** importieren, wird der Schlüssel erstellt. Klicken Sie auf **Beenden**. Der Vorgang ist abgeschlossen.
   - Wenn Sie das Zertifikat mit der Option **Als PGP X.509-Wrapper-Schlüssel** importieren, wird das Dialogfeld „Schlüssel auswählen“ angezeigt. Wählen Sie den Schlüssel per Mausklick aus und klicken Sie auf „Importieren“. Der PGP X.509-Wrapper-Schlüssel wird erstellt. Der Vorgang ist abgeschlossen.
5. Wählen Sie zum Abschließen des Zertifikatimports mit der Option **Auf einen vorhandenen Schlüssel** im Dialogfeld **Schlüssel auswählen** den Schlüssel aus, in den das Zertifikat importiert werden soll. Geben Sie dann die Passphrase für den Schlüssel ein. Klicken Sie auf **Weiter**.

6 Das Dialogfeld „Fortschritt der Schlüsselerstellung“ wird angezeigt, während das Zertifikat in den Schlüssel importiert wird.

7 Klicken Sie auf **Beenden**. Der Vorgang ist abgeschlossen.

Passphrase ändern

Es empfiehlt sich, die Passphrase regelmäßig zu ändern, z. B. alle drei Monate. Noch wichtiger ist es, die Passphrase sofort zu ändern, wenn Sie vermuten, dass die Sicherheit gefährdet ist, z. B. wenn Ihnen jemand während der Eingabe über die Schulter geblickt hat.

Damit Sie die Passphrase eines geteilten Schlüssels ändern können, müssen Sie diesen zuerst wieder zusammenfügen.

Tipp: Wenn Sie die Passphrase des Schlüssels ändern, wird die Passphrase von Kopien des Schlüssels (z. B. Sicherungskopien) nicht geändert. Wenn Sie annehmen, dass die Passphrase nicht mehr geheim ist, empfiehlt die PGP Corporation, alle Sicherungskopien sicher zu löschen und neue Sicherungskopien des Schlüssels zu erstellen.

Wenn Sie in einer von einem PGP Universal Server verwalteten Umgebung arbeiten und den SKM-Schlüsselmodus verwenden, können Sie die Passphrase des Schlüssels nicht ändern. SKM-Schlüssel werden durch eine auf Zufallsbasis erzeugte Passphrase geschützt (die wiederum selbst geschützt ist) und Sie werden nie aufgefordert, eine Passphrase für einen SKM-Schlüssel einzugeben. Informationen zum Ermitteln des Schlüsselmodus finden Sie unter *Schlüsselmodi* (auf Seite 136).

So ändern Sie die Passphrase des privaten Schlüssels

1 Öffnen Sie PGP Desktop, klicken Sie auf das Bedienfeld „PGP-Schlüssel“ und wählen Sie **Eigene privaten Schlüssel** aus.

2 Doppelklicken Sie im Arbeitsbereich „PGP Keys“ auf den privaten Schlüssel, dessen Passphrase Sie ändern möchten. Das Dialogfeld „Schlüsseleigenschaften“ wird angezeigt.

3 Klicken Sie auf **Passphrase ändern**. Der Assistent für PGP-Passphrasen wird angezeigt.

4 Geben Sie die aktuelle Passphrase des privaten Schlüssels ein und klicken Sie auf **Weiter**.Das Dialogfeld „Passphrase erstellen“ wird angezeigt.

5 Geben Sie die neue Passphrase im ersten Textfeld ein und wiederholen Sie die Eingabe zur Bestätigung im Feld **Passphrase erneut eingeben**.

Wenn die Zeichen der Passphrase während der Eingabe angezeigt werden sollen, aktivieren Sie das Kontrollkästchen **Tastatureingabe anzeigen**.

Die Passphrasen-Qualitätsanzeige gibt Ihnen eine Richtlinie für die Stärke der Passphrase, die Sie erstellen. Sie vergleicht den Entropiewert der eingegebenen Passphrase mit einer echten zufälligen Zeichenkette mit 128 Bit (der gleiche Entropiewert wie in einem AES128-Schlüssel). Weitere Informationen finden Sie unter *Passphrasen-Qualitätsanzeige* (siehe "Die Passphrasen-Qualitätsanzeige" auf Seite 352).

6 Klicken Sie auf **Fertig stellen**.Die Passphrase wurde geändert.

Schlüssel, Benutzer-IDs und Signaturen löschen

PGP Desktop gibt Ihnen die Kontrolle über die Schlüssel an Ihren Schlüsselbunden sowie über die Benutzer-IDs und Signaturen an diesen Schlüsseln.

Bei öffentlichen Schlüsseln an Ihren Schlüsselbunden können Sie ganze Schlüssel, beliebige Benutzer-IDs an einem Schlüssel und beliebige oder alle Signaturen an einem Schlüssel löschen.

Bei Ihren Schlüsselpaaren können Sie ganze Schlüsselpaare oder beliebige Signaturen löschen. Sie können auch Benutzer-IDs aus einem Schlüsselpaar löschen, falls es sich nicht um die einzige Benutzer-ID des Schlüsselpaars handelt.

Beachten Sie jedoch, dass Sie die Benutzer-ID nicht aus einem Schlüssel löschen können, wenn es sich hierbei um die einzige Benutzer-ID handelt. Auch Autosignaturen können nicht von Schlüsseln gelöscht werden.

So löschen Sie einen Schlüssel, eine Benutzer-ID oder eine Signatur vom PGP-Schlüsselbund

1 Öffnen Sie PGP Desktop, klicken Sie auf das Bedienfeld „PGP-Schlüssel“ und klicken Sie im Bedienfeld auf **Alle Schlüssel**. Alle Schlüssel am Schlüsselbund werden angezeigt.

2 Führen Sie einen der folgenden Schritte aus:

- Um einen Schlüssel zu löschen, klicken Sie mit der rechten Maustaste auf den Schlüssel, wählen Sie **Löschen** aus der angezeigten Liste der Befehle aus und klicken Sie im Bestätigungsdialogfeld auf **OK**. Der Schlüssel wird aus dem Schlüsselbund gelöscht.
- Um eine Benutzer-ID (von einem öffentlichen Schlüssel) oder um eine Signatur zu löschen, klicken Sie auf das Pluszeichen links neben dem Schlüssel, um die Benutzer-IDs und Signaturen anzuzeigen. Wenn Sie die Benutzer-ID oder Signatur sehen, die Sie löschen wollen, klicken Sie mit der rechten Maustaste darauf, wählen Sie **Löschen** aus der angezeigten Liste der Befehle aus, und klicken Sie dann im Bestätigungs-Dialogfeld auf **OK**. Die Benutzer-ID oder Signatur wird gelöscht.

Öffentliche Schlüssel deaktivieren und aktivieren

In bestimmten Situationen möchten Sie möglicherweise einen öffentlichen Schlüssel am Schlüsselbund vorübergehend deaktivieren. Dies trifft beispielsweise zu, wenn Sie einen öffentlichen Schlüssel zwar für die künftige Verwendung behalten möchten, der Schlüssel jedoch nicht bei jeder versendeten E-Mail-Nachricht in die Empfängerliste aufgenommen werden soll.

Sie können keine Schlüsselpaare deaktivieren, die implizit vertrauenswürdig sind. Wenn Sie einen Schlüssel deaktivieren möchten, der als implizit vertrauenswürdig eingestuft wurde, müssen Sie zuerst den Vertrauensstatus auf **Keine** ändern.

So deaktivieren oder aktivieren Sie einen öffentlichen Schlüssel

1. Öffnen Sie PGP Desktop, klicken Sie auf das Bedienfeld „PGP-Schlüssel“ und klicken Sie im Bedienfeld auf **Alle Schlüssel**. Alle Schlüssel am Schlüsselbund werden angezeigt.
2. Doppelklicken Sie auf den öffentlichen Schlüssel, den Sie deaktivieren möchten. Das Dialogfeld „Schlüsseleigenschaften“ wird für den ausgewählten Schlüssel angezeigt.
3. Suchen Sie in den Schlüsseleigenschaften das Feld **Aktiviert**.
   - Wenn derzeit für die Einstellung **Aktiviert** die Option **Ja** ausgewählt ist, ist der Schlüssel aktiviert. Wenn Sie den Schlüssel deaktivieren möchten, klicken Sie einmal auf **Ja**. Im Feld **Aktiviert** wird jetzt die Option **Nein** angezeigt. Der Schlüssel ist deaktiviert.
   - Wenn derzeit für die Einstellung **Aktiviert** die Option **Nein** ausgewählt ist, ist der Schlüssel deaktiviert. Wenn Sie den Schlüssel aktivieren möchten, klicken Sie einmal auf **Nein**. Im Feld **Aktiviert** wird die Option **Ja** angezeigt. Der Schlüssel ist also aktiviert.

Ein deaktivierter Schlüssel kann nicht zum Verschlüsseln oder Signieren verwendet werden. Sie können einen deaktivierten Schlüssel jedoch zum Entschlüsseln oder Verifizieren verwenden.

Tipp: Sie können Schlüssel an Ihrem Schlüsselbund auch mit dem PGP Universal Server synchronisieren. Diese Option wird in erster Linie zum Aktivieren bzw. Deaktivieren öffentlicher Schlüssel am Schlüsselbund verwendet. Klicken Sie hierzu mit der rechten Maustaste auf einen Schlüssel und wählen Sie **Synchronisieren** aus.

Einen öffentlichen Schlüssel verifizieren

Es ist schwer zu wissen, ob ein öffentlicher Schlüssel einer bestimmten Person gehört, sofern Sie den Schlüssel nicht direkt von der betreffenden Person auf einem Datenträger erhalten oder vom PGP Global Directory abrufen. Das Austauschen von Schlüsseln auf Datenträgern bietet sich in der Regel nicht an, besonders für Benutzer, die sich nicht am selben Ort befinden.

Daher stellt sich die Frage, wie sichergestellt werden kann, dass der öffentliche Schlüssel, der von einem öffentlichen Keyserver (nicht vom PGP Global Directory) abgerufen wurde, tatsächlich der öffentliche Schlüssel der Person ist, die auf dem Schlüssel aufgeführt ist? Die Lösung ist, dass Sie den Fingerabdruck des Schlüssels überprüfen müssen

Sie haben mehrere Möglichkeiten, den Fingerabdruck eines Schlüssels zu überprüfen. Es ist aber am sichersten, wenn Sie die Person anrufen und sich den Fingerabdruck am Telefon vorlesen lassen. Falls die Person nicht das Ziel eines Angriffs ist, ist es äußerst unwahrscheinlich, dass jemand dieses zufällige Gespräch abhört und sich als die Person ausgibt, die Sie am anderen Ende der Leitung erwarten. Sie können auch den Fingerabdruck auf Ihrer Kopie des öffentlichen Schlüssels einer Person mit dem Fingerabdruck des Originalschlüssels dieser Person auf einem öffentlichen Server vergleichen.

Der Fingerabdruck kann auf zwei Arten angezeigt werden: in einer eindeutigen Wortliste oder im Hexadezimal-Format.

So überprüfen Sie den digitalen Fingerabdruck auf einem öffentlichen Schlüssel

1. Öffnen Sie PGP Desktop, klicken Sie auf das Bedienfeld „PGP-Schlüssel“ und klicken Sie im Bedienfeld auf **Alle Schlüssel**.

   Alle Schlüssel am Schlüsselbund werden angezeigt.

2. Doppelklicken Sie auf den öffentlichen Schlüssel, dessen Fingerabdruck Sie prüfen wollen. Das Dialogfeld „Schlüsseleigenschaften“ wird für den ausgewählten Schlüssel angezeigt.

   Der Fingerabdruck des Schlüssels wird unter dem Namen und der E-Mail-Adresse im Hexadezimal-Format (10 Gruppen zu je vier Zeichen) oder im Wortlistenformat (vier Spalten mit je fünf eindeutigen Wörtern) angezeigt.

3. Vergleichen Sie den Fingerabdruck auf dem Schlüssel mit dem Original-Fingerabdruck. Wenn die beiden Codes übereinstimmen, besitzen Sie den echten Schlüssel. Ist dies nicht der Fall, besitzen Sie *nicht* den echten Schlüssel.

   Die Wortliste besteht aus bestimmten, von PGP Desktop verwendeten Authentifizierungswörtern. Die Wörter wurden sorgfältig ausgewählt, um phonetisch unterscheidbar und unmissverständlich zu sein.

Die Wortliste erfüllt einen ähnlichen Zweck wie das Funkalphabet, mit dem Piloten Informationen über Funkkanäle mit Störgeräuschen übermitteln können.

4 Falls der Schlüssel gefälscht ist, löschen Sie ihn.

5 Öffnen Sie einen Webbrowser, rufen Sie das *PGP Global Directory* (https://keyserver.pgp.com) auf und suchen Sie nach dem echten öffentlichen Schlüssel.

Öffentliche Schlüssel signieren

Wenn Sie ein Schlüsselpaar erstellen, werden die Schlüssel automatisch signiert. Entsprechend können Sie den öffentlichen Schlüssel einer anderen Person signieren, wenn Sie sicher sind, dass es sich um den Schlüssel dieser Person handelt. Dadurch geben Sie an, dass Sie den Schlüssel verifiziert haben. Wenn Sie den öffentlichen Schlüssel einer Person signieren, wird der Schlüssel zusammen mit einem Signatursymbol und Ihrem Benutzernamen angezeigt.

Falls Sie ein Schlüsselpaar von einer Sicherungsdatei oder von einem anderen Rechner importieren, muss dieses Schlüsselpaar u. U. auch signiert werden.

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, ist die Schlüsselsignierung möglicherweise deaktiviert.

So signieren Sie den Schlüssel einer anderen Person

1 Öffnen Sie PGP Desktop, klicken Sie auf das Bedienfeld „PGP-Schlüssel“ und klicken Sie im Bedienfeld auf **Alle Schlüssel**. Alle Schlüssel am Schlüsselbund werden angezeigt.

2 Führen Sie einen der folgenden Schritte aus:

- Klicken Sie im Menü **Schlüssel** auf **Signieren**.
- Klicken Sie mit der rechten Maustaste auf den Schlüssel, den Sie signieren möchten, und wählen Sie aus der Liste der angezeigten Befehle die Option **Signieren** aus.

Das Dialogfeld „PGP-Signaturschlüssel“ wird geöffnet, wobei der Benutzername bzw. die E-Mail-Adresse und der Hexadezimal-Fingerabdruck im Textfeld angezeigt werden.

3 Aktivieren Sie das Kontrollkästchen **Export der Signatur zulassen**, damit die Signatur mit diesem Schlüssel exportiert werden kann.

Eine exportierbare Signatur kann an Server gesendet werden und wird immer mit dem Schlüssel mitgesendet, wenn dieser exportiert wird, z. B. wenn er in eine E-Mail-Nachricht gezogen wird. Mit diesem Kontrollkästchen können Sie einfach angeben, dass die Signatur exportiert werden soll, damit andere sich auf Ihre Signatur verlassen und daher Ihren Schlüsseln vertrauen können.

4. Klicken Sie auf **Weitere Optionen**, um Optionen wie den Signaturtyp und das Ablaufdatum der Signatur zu konfigurieren.
5. Wählen Sie einen Signaturtyp zum Signieren des öffentlichen Schlüssels aus. Folgende Optionen sind verfügbar:
   - **Nicht exportierbar:** Verwenden Sie diesen Signaturtyp, wenn der Schlüssel Ihrer Meinung nach gültig ist, Sie jedoch nicht möchten, dass sich andere Personen auf Ihre Zertifizierung verlassen. Dieser Signaturtyp kann nicht mit dem zugehörigen Schlüssel an einen Keyserver gesendet oder auf andere Art exportiert werden.
   - **Exportierbar:** Verwenden Sie exportierbare Signaturen, wenn Ihre Signatur mit dem Schlüssel an den Keyserver gesendet wird, damit andere sich auf Ihre Signatur verlassen und daher Ihren Schlüsseln vertrauen können. Diese Vorgehensweise entspricht dem Aktivieren des Kontrollkästchens **Export der Signatur zulassen** im Menü Schlüssel signieren.
   - **Meta-Vertrauensperson, nicht exportierbar:** Mit dieser Option wird bestätigt, dass dieser Schlüssel und alle Schlüssel, die durch diesen Schlüssel als Vertrauensperson signiert wurden, als Vertrauenspersonen akzeptiert wurden, die wiederum Schlüssel signieren können, die Sie automatisch als vertrauenswürdig einstufen. Dieser Signaturtyp ist nicht exportierbar.
   - **Vertrauensperson, exportierbar:** Verwenden Sie diese Signatur, wenn Sie bestätigen möchten, dass dieser Schlüssel gültig ist und dass dem Besitzer des Schlüssels vollkommen vertraut werden soll, wenn dieser sich für andere Schlüssel verbürgt. Dieser Signaturtyp ist exportierbar. Sie können die Validierungsmöglichkeiten der Vertrauensperson auf eine bestimmte E-Mail-Domäne beschränken.
6. Über die Option **Maximale Vertrauenstiefe** können Sie die Anzahl der Ebenen angeben, bis zu der Vertrauenspersonen verschachtelt werden können. Falls Sie beispielsweise den Wert 1 auswählen, kann nur eine Ebene von Vertrauenspersonen unter dem Schlüssel der Meta-Vertrauensperson liegen.
7. Falls Sie die Möglichkeit für die Schlüsselvalidierung der Vertrauensperson auf eine einzige Domäne beschränken möchten, geben Sie den Domänennamen in das Textfeld **Domäneneinschränkung** ein.
8. Wählen Sie im Feld **Ablaufdatum** die Option **Nie** aus, wenn diese Signatur nie ablaufen soll. Geben Sie andernfalls ein Ablaufdatum an.
9. Klicken Sie auf **OK.** Das Dialogfeld „PGP-Passphrase für Schlüssel eingeben“ wird angezeigt.

10 Wählen Sie in der Liste den Schlüssel aus, den Sie zum Signieren verwenden möchten, und geben Sie bei Bedarf die Passphrase des Signaturschlüssels ein. (Falls die Passphrase bereits zwischengespeichert wurde, müssen Sie sie nicht erneut eingeben.)

11 Klicken Sie auf **OK.** Der Schlüssel ist signiert.

Signaturen von öffentlichen Schlüsseln widerrufen

Unter Umständen kann es erforderlich oder wünschenswert sein, Ihre Signatur von einem Schlüssel am Schlüsselbund zu widerrufen.

▸ **So widerrufen Sie Ihre Signatur**

1 Öffnen Sie PGP Desktop, klicken Sie auf das Bedienfeld „PGP-Schlüssel“ und klicken Sie im Bedienfeld auf **Alle Schlüssel**. Alle Schlüssel am Schlüsselbund werden angezeigt.

2 Erweitern Sie den Schlüssel, dessen Signatur Sie widerrufen möchten, bis Sie Ihren Signaturschlüssel sehen.

3 Klicken Sie mit der rechten Maustaste auf Ihren Signaturschlüssel und wählen Sie dann aus der angezeigten Befehlsliste **Widerrufen** aus. Das Dialogfeld Signatur widerrufen wird angezeigt.

4 Überprüfen Sie, ob die Schlüssel-ID und der Name des richtigen Schlüssels (von dem Sie die Signatur widerrufen möchten) angezeigt werden und klicken Sie auf **OK**. Das Dialogfeld „PGP-Passphrase für Schlüssel eingeben“ wird angezeigt.

5 Geben Sie die Passphrase ein und klicken Sie auf **OK**. Ihre Signatur des Schlüssels wird widerrufen.

Hinweis: Wenn Ihre Signatur exportierbar war und Sie den Schlüssel mit der exportierbaren Signatur verteilt haben, müssen Sie auch den Schlüssel mit der widerrufenen Signatur verteilen, damit andere Personen das Widerrufen sehen können.

Vertrauen für Schlüsselvalidierungen gewähren

Sie können nicht nur bestätigen, dass ein Schlüssel einer bestimmten Person gehört, sondern haben auch die Möglichkeit, dem Eigentümer des Schlüssels eine Vertrauensstufe zuzuweisen, die angibt, wie sehr Sie ihm in seiner Rolle als Vertrauensperson für Schlüssel anderer Personen vertrauen, die Sie in Zukunft erhalten mögen.

Dies bedeutet, dass jeder Schlüssel, den Sie erhalten, als gültig eingeschätzt wird, falls er von einer Person signiert wurde, die Sie als vertrauenswürdig bestätigt haben, selbst wenn Sie die Gültigkeit nicht selbst überprüft haben.

Sie müssen einen Schlüssel signieren, bevor Sie eine Vertrauensstufe dafür festlegen können.

Für öffentliche Schlüssel sind die Optionen **Keine**, **Marginal** und **Vertrauenswürdig** verfügbar. Vertrauenseinstellungen für Schlüsselpaare lauten **Keine** oder **Implizit** (d. h. dass es sich um Ihren eigenen Schlüssel handelt und Sie diesem vollständig vertrauen). Sie sollten nicht im Besitz von Schlüsselpaaren anderer Personen sein.

Weitere Informationen zu vertrauenswürdigen Schlüsseln finden Sie unter *Einführung in die Kryptografie*.

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, ist die Möglichkeit, einen Schlüssel als vertrauenswürdig einzustufen, möglicherweise deaktiviert.

So stufen Sie einen Schlüssel als vertrauenswürdig ein

1. Öffnen Sie PGP Desktop, klicken Sie auf das Bedienfeld „PGP-Schlüssel“ und klicken Sie im Bedienfeld auf **Alle Schlüssel**. Alle Schlüssel am Schlüsselbund werden angezeigt.
2. Doppelklicken Sie auf den Schlüssel, den Sie als vertrauenswürdig einstufen möchten. Das Dialogfeld „Schlüsseleigenschaften“ wird für den ausgewählten Schlüssel angezeigt.
3. Gehen Sie zum Feld **Vertrauen.**
4. Klicken Sie auf die aktuelle Einstellung und wählen Sie die gewünschte Einstellung aus der Liste aus.
   - Falls Sie einem öffentlichen Schlüssel eine Vertrauensstufe zuweisen, können Sie zwischen **Keine**, **Marginal** und **Vertrauenswürdig** wählen. „Keine“ bedeutet, dass Sie dem Besitzer als Vertrauensperson nicht vertrauen, „Marginal“ bedeutet, dass Sie ihm teilweise vertrauen, „Vertrauenswürdig“ bedeutet, dass Sie ihm voll vertrauen.
   - Falls Sie einem Schlüsselpaar eine Vertrauensstufe zuweisen, können Sie zwischen **Keine** und **Implizit** auswählen. Die Vertrauenswürdigkeit muss nur für Schlüsselpaare, die Sie von einer Sicherungsdatei oder von einem anderen Computer importieren, auf „Implizit“ gesetzt werden. Wenn Sie ein Schlüsselpaar erstellen, wird die Vertrauenswürdigkeit automatisch auf „Implizit“ gesetzt.

Mit Unterschlüsseln arbeiten

Ein Schlüsselpaar von PGP Desktop besteht aus folgenden Elementen:

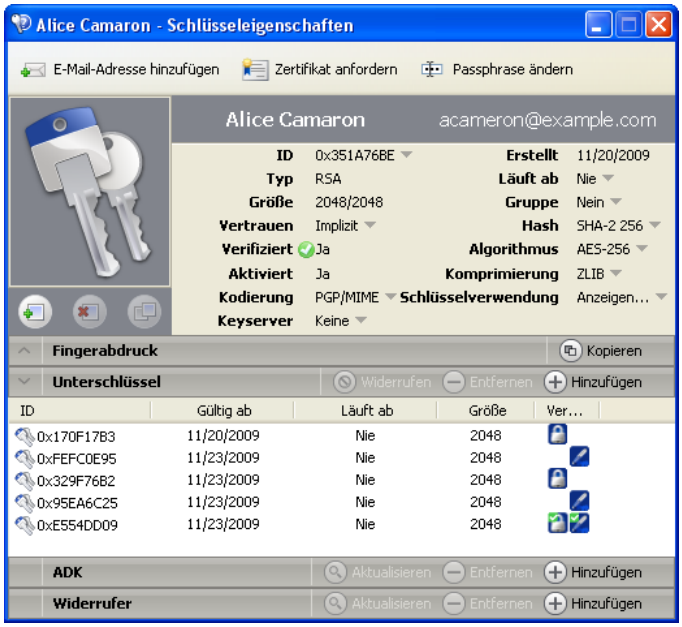
- Dem **Hauptschlüssel**, der nur zum Signieren verwendet wird

- Einem obligatorischen **Unterschlüssel für die Verschlüsselung**
- Einem oder mehreren *optionalen* **separaten Unterschlüsseln** zum Signieren, Verschlüsseln oder Signieren/Verschlüsseln

Der Hauptschlüssel wird standardmäßig zum Signieren verwendet, während ein Unterschlüssel immer zur Verschlüsselung verwendet wird. Dadurch kann die Sicherheit eines PGP Desktop-Schlüsselpaars verbessert werden, da ein separater Unterschlüssel für die Verschlüsselung widerrufen, entfernt oder einem PGP Desktop-Schlüsselpaar hinzugefügt werden kann, ohne Auswirkungen auf den Hauptschlüssel oder die darin enthaltenen Signaturen zu haben.

Neben dem Hauptschlüssel und dem obligatorischen Unterschlüssel für die Verschlüsselung können Sie zusätzliche Unterschlüssel für Ihr PGP Desktop-Schlüsselpaar erstellen. Sie können verschiedenste Kombinationen für Unterschlüssel erstellen, die nur zur Verschlüsselung, nur zum Signieren oder sowohl zum Verschlüsseln als auch zum Signieren verwendet werden können.

Zeigen Sie die Unterschlüssel eines Schlüsselpaars im Dialogfeld „Schlüsseleigenschaften“ an. In der Spalte „Verwendung“ wird die Funktion des Unterschlüssels angegeben:



Schlüssel	Beschreibung
	Unterschlüssel für die Verschlüsselung weisen ein blaues Schlosssymbol auf.
	Signatur-Unterschlüssel weisen ein blaues Stiftsymbol auf.
	Unterschlüssel, die sowohl zum Verschlüsseln als

Schlüssel	Beschreibung
	auch zum Signieren verwendet werden, weisen beide Symbole auf.
	Der standardmäßige Unterschlüssel für die Verschlüsselung weist oben links ein kleines grünes Häkchen auf.
	Der standardmäßige Signatur-Unterschlüssel weist oben links ein kleines grünes Häkchen auf.

Separate Unterschlüssel verwenden

Einige Beispiele für die sinnvolle Verwendung von zusätzlichen separaten Unterschlüsseln:

- **Mehrere Unterschlüssel**, die zur Verschlüsselung verwendet werden und in verschiedenen Phasen der Funktionsdauer eines Schlüsselpaars gültig sind, können einen Sicherheitsgewinn erreichen. Sie können für die Verschlüsselung Unterschlüssel erstellen, deren Start- und Ablaufdaten so gelegt sind, dass jeweils immer nur ein Unterschlüssel gilt. So können Sie beispielsweise mehrere Unterschlüssel erstellen, die jeweils nur für ein Jahr gelten. (Achten Sie dabei auf die Datumsübergänge.) Der Unterschlüssel für die Verschlüsselung wechselt dann jährlich. Dies kann eine nützliche Sicherheitsmaßnahme sein und bietet sich als automatisierte Methode zum regelmäßigen Wechseln des Unterschlüssels für die Verschlüsselung an, da dabei kein neuer öffentlicher Schlüssel erstellt und verteilt werden muss. Abgelaufene Unterschlüssel sind an einem Schlüsselsymbol mit einer roten Uhr zu erkennen.
- **Separate Signatur-Unterschlüssel** sind in Ländern und Regionen erforderlich, in denen separate Unterschlüssel für rechtsgültige digitale Signaturen vorgeschrieben sind.

Welche separaten Unterschlüssel Sie erstellen können, richtet sich nach dem Typ des Schlüsselpaars, mit dem Sie arbeiten:

- Für RSA-Schlüsselpaare können Sie Unterschlüssel allein zum Verschlüsseln, allein zum Signieren oder zum Verschlüsseln und Signieren erstellen.
- Für Diffie-Hellman/DSS-Schlüsselpaare können Sie Unterschlüssel allein zum Verschlüsseln oder allein zum Signieren erstellen, nicht jedoch zum kombinierten Verschlüsseln und Signieren.
- Unterschlüssel werden für ältere PGP-Legacy-Schlüsselpaare nicht unterstützt.

Unterschlüssel anzeigen

Sie können die Informationen zu den Unterschlüsseln auf Ihren eigenen Schlüsselpaaren anzeigen und ändern. Die Informationen zu den Unterschlüsseln auf den öffentlichen Schlüsselpaaren Ihres Schlüsselbunds können nur angezeigt, aber nicht geändert werden.

So zeigen Sie Unterschlüssel und ihre Eigenschaften an

1. Öffnen Sie PGP Desktop, klicken Sie auf das Bedienfeld „PGP-Schlüssel“ und klicken Sie auf **Alle Schlüssel**.

   Alle Schlüssel am Schlüsselbund werden angezeigt.

2. Sie haben mehrere Möglichkeiten, die Eigenschaften eines Schlüssels anzuzeigen:

   - Doppelklicken Sie auf den Schlüssel, dessen Eigenschaften Sie anzeigen möchten.
   - Klicken Sie mit der rechten Maustaste auf den Schlüssel und wählen Sie im Kontextmenü die Option **Schlüsseleigenschaften** aus.
   - Wählen Sie den Schlüssel im Schlüsselbund aus und klicken Sie dann auf **Schlüssel > Schlüsseleigenschaften**.

   Das Dialogfeld „Schlüsseleigenschaften“ wird für den ausgewählten Schlüssel angezeigt.

3. Klicken Sie im Dialogfeld „Schlüsseleigenschaften“ auf die Überschrift **Unterschlüssel**. Die Unterschlüssel für diesen Schlüssel werden angezeigt.

4. Wenn Sie die Eigenschaften eines Unterschlüssels anzeigen möchten, klicken Sie mit der rechten Maustaste auf den Unterschlüssel, den Sie anzeigen möchten, und wählen Sie im Kontextmenü die Option **Unterschlüsseleigenschaften** aus.

Neue Unterschlüssel erstellen

Wahrscheinlich werden Sie neue Unterschlüssel entsprechend der Anleitungen in diesem Abschnitt erstellen. Sie können Unterschlüssel jedoch auch bei der ersten Installation von PGP Desktop mit dem Assistenten für die Erstellung neuer Schlüssel erstellen. Weitere Informationen finden Sie unter *PGP Desktop erstmals verwenden* (auf Seite 18).

So erstellen Sie neue Unterschlüssel

1. Klicken Sie im Dialogfeld „Schlüsseleigenschaften“ im Bereich „Unterschlüssel“ auf die Schaltfläche **Hinzufügen**. Das Dialogfeld „Neuer Unterschlüssel“ wird angezeigt.

2 Wählen Sie im Bereich **Diesen Schlüssel verwenden für** die Option **Verschlüsselung**, **Signieren oder Verschlüsselung und Signieren** aus. Die Auswahl hängt von der geplanten Verwendung des neuen Unterschlüssels ab.

3 Wählen Sie im Feld **Schlüsselgröße** eine Schlüsselgröße zwischen 1024 und 4096 Bit aus oder geben Sie eine benutzerdefinierte Schlüsselgröße zwischen 1024 und 4096 Bit ein.

4 Geben Sie im Feld **Startdatum** ein Datum ein, an dem der neue Unterschlüssel in Kraft tritt, oder wählen Sie ein Datum aus dem Kalender aus.

5 Wählen Sie im Bereich **Ablaufdatum** die Option **Nie** aus oder wählen Sie **Datum** und legen Sie ein Datum fest. Sie können auch im Kalender ein Datum auswählen. Diese Angaben legen fest, wann der Unterschlüssel abläuft.

6 Klicken Sie auf **OK.** Das Passphrasen-Dialogfeld wird angezeigt.

7 Geben Sie die Passphrase ein und klicken Sie auf **OK**.Der Unterschlüssel wird erstellt.

Informationen zum Festlegen der Verwendung des Schlüssels (z. B. nur für PGP Messaging) finden Sie unter *Schlüsselverwendung für Unterschlüssel festlegen* (auf Seite 79).

Schlüsselverwendung für Unterschlüssel festlegen

Jeder Unterschlüssel kann eigene Eigenschaften für die Schlüsselverwendung aufweisen. Zum Beispiel könnte ein Unterschlüssel nur für PGP Whole Disk Encryption und ein anderer für alle anderen Funktionen von PGP Desktop verwendet werden.

Es bietet sich beispielsweise an, die Schlüsselverwendung eines Schlüssels festzulegen, wenn Sie einen Schlüssel ausschließlich zur Laufwerksverschlüsselung und nicht zum Empfangen von verschlüsselten E-Mail-Nachrichten verwenden möchten. Wenn Sie einen öffentlichen Schlüssel verteilen, der PGP Messaging nicht zulässt, werden von einem anderen Benutzer gesendete E-Mail-Nachrichten nicht an Ihren öffentlichen Schlüssel verschlüsselt.

Hinweis: Wenn Sie in einer von einem PGP Universal Server verwalteten Umgebung arbeiten und den SKM-Schlüsselmodus verwenden, können Sie keine Änderungen an den Markierungen für die Schlüsselverwendung vornehmen. Informationen zum Ermitteln des Schlüsselmodus finden Sie unter *Schlüsselmodi* (auf Seite 136).

So legen Sie die Schlüsselverwendung fest

1 Öffnen Sie PGP Desktop, klicken Sie auf das Bedienfeld „PGP-Schlüssel“ und klicken Sie auf **Alle Schlüssel**.

Alle Schlüssel am Schlüsselbund werden angezeigt.

2 Sie haben mehrere Möglichkeiten, die Eigenschaften eines Schlüssels anzuzeigen:

- Doppelklicken Sie auf den Schlüssel, dessen Eigenschaften Sie anzeigen möchten.
- Klicken Sie mit der rechten Maustaste auf den Schlüssel und wählen Sie im Kontextmenü die Option **Schlüsseleigenschaften** aus.
- Wählen Sie den Schlüssel im Schlüsselbund aus und klicken Sie dann auf **Schlüssel > Schlüsseleigenschaften**.

Das Dialogfeld „Schlüsseleigenschaften“ wird für den ausgewählten Schlüssel angezeigt.

3 Klicken Sie im Dialogfeld „Schlüsseleigenschaften“ auf die Überschrift **Unterschlüssel**. Die Unterschlüssel für diesen Schlüssel werden angezeigt.

4 Wenn Sie die Eigenschaften eines Unterschlüssels anzeigen möchten, klicken Sie mit der rechten Maustaste auf den Unterschlüssel, den Sie anzeigen möchten, und wählen Sie im Kontextmenü die Option **Unterschlüsseleigenschaften** aus.

5 Wählen Sie unter „Schlüsselverwendung“ die PGP Desktop-Funktionen aus, für die dieser Schlüssel verwendet werden kann. Durch ein Häkchen neben dem Objekt wird angezeigt, dass der Schlüssel für diese Funktion verwendet werden kann.

6 Klicken Sie auf **Schließen**, um die Unterschlüsseleigenschaften zu speichern.

Unterschlüssel widerrufen

▸ **So widerrufen Sie einen Unterschlüssel**

1. Wählen Sie im Dialogfeld „Schlüsseleigenschaften“ im Bereich **Unterschlüssel** den Unterschlüssel aus, den Sie widerrufen möchten. Klicken Sie anschließend auf **Widerrufen** (über der Liste der Unterschlüssel). Sie werden in einem PGP-Warndialogfeld **darauf hingewiesen, dass andere Benutzer nach dem Widerrufen des Unterschlüssels keine Daten mehr an diesen Schlüssel verschlüsseln können.**
2. Klicken Sie auf **Ja**, um den Unterschlüssel zu widerrufen, oder auf **Nein**, um den Vorgang abzubrechen. Das Passphrasen-Dialogfeld wird angezeigt.
3. Geben Sie die Passphrase ein und klicken Sie auf **OK**. Der Unterschlüssel wird widerrufen und das Symbol ändert sich.

Unterschlüssel entfernen

▸ **So entfernen Sie einen Unterschlüssel**

1. Wählen Sie im Dialogfeld **Schlüsseleigenschaften** im Bereich **Unterschlüssel** den Unterschlüssel aus, den Sie entfernen möchten. Klicken Sie anschließend auf **Entfernen** (über der Liste der Unterschlüssel). Sie werden in einem PGP-Warndialogfeld **darauf hingewiesen, dass Sie nach dem Entfernen des Unterschlüssels keine Daten mehr entschlüsseln können, die an diesen Unterschlüssel verschlüsselt sind.**
2. Klicken Sie auf **Ja**, um den Unterschlüssel zu entfernen, oder auf **Nein**, um den Vorgang abzubrechen. Der Unterschlüssel wird entfernt.

Mit ADKs arbeiten

Additional Decryption Keys (ADKs) sind Schlüssel, die von Sicherheitsbeauftragten in Organisationen zum Entschlüsseln von Nachrichten eingesetzt werden, die Mitarbeiter in der Organisation empfangen oder gesendet haben.

Nachrichten, die an einen Schlüssel mit einem ADK verschlüsselt sind, werden an den öffentlichen Schlüssel des Empfängers sowie an den ADK verschlüsselt. Der Inhaber des ADK kann die Nachricht also ebenfalls entschlüsseln.

ADK werden selten außerhalb einer von einem PGP Universal Server verwalteten Umgebung eingesetzt oder benötigt. Obwohl der PGP-Administrator im Regelfall keinen Bedarf für die Anwendung von Additional Decryption Keys hat, gibt es Umstände, die die Wiederherstellung der E-Mail-Nachrichten anderer Personen erforderlich machen. Dieser Fall kann z. B. eintreten, wenn ein Mitarbeiter längere Zeit krank ist oder wenn E-Mail-Aufzeichnungen auf behördliche Anordnung vorgelegt werden müssen und das Unternehmen E-Mail-Nachrichten für die Beweiserbringung in einem Gerichtsverfahren entschlüsseln muss.

Sie können nur ADKs an Ihren Schlüsselpaaren ändern.

ADKs zu einem Schlüsselpaar hinzufügen

So fügen Sie einen ADK hinzu

1. Öffnen Sie PGP Desktop, klicken Sie auf das Bedienfeld „PGP Keys“ und dann auf **Eigene private Schlüssel**. Die privaten Schlüssel am Schlüsselbund werden angezeigt.
2. Doppelklicken Sie auf den Schlüssel, dem Sie einen ADK hinzufügen möchten. Das Dialogfeld „Schlüsseleigenschaften“ für den von Ihnen ausgewählten Schlüssel wird angezeigt.
3. Klicken Sie links neben **ADK** auf den Pfeil nach oben (der Pfeil ist nur bei Schlüsseln vorhanden, denen bereits ein ADK zugewiesen wurde). Die ADK-Informationen für diesen Schlüssel werden angezeigt (falls konfiguriert).
4. Klicken Sie auf das Plussymbol rechts neben dem ADK-Bereich. Das Dialogfeld „Schlüssel auswählen“ wird angezeigt.
5. Wählen Sie den Schlüssel aus, den Sie als ADK verwenden möchten, und klicken Sie auf **OK**. Sie werden in einem PGP-Warndialogfeld aufgefordert, das Hinzufügen des ausgewählten Schlüssels als ADK zu bestätigen.
6. Klicken Sie auf **Ja**. Das Dialogfeld „PGP-Passphrase für Schlüssel eingeben“ wird angezeigt.
7. Geben Sie die Passphrase für den Schlüssel ein, dem Sie den ADK hinzufügen möchten, und klicken Sie auf **OK**. Das Dialogfeld „PGP-Informationen“ wird angezeigt und Sie werden darüber informiert, dass der ADK dem Schlüssel hinzugefügt wurde.
8. Klicken Sie auf **OK**.

Hinweis: Wenn Sie Ihrem Schlüssel einen ADK hinzufügen, müssen die Personen, die Ihnen verschlüsselte E-Mail-Nachrichten senden, Zugriff auf den öffentlichen Schlüssel des ADK haben.

Einen ADK aktualisieren

So aktualisieren Sie einen ADK

1. Wählen Sie den ADK, den Sie aktualisieren möchten, in der Liste der ADKs aus. Der ausgewählte ADK wird markiert.
2. Klicken Sie auf das Symbol mit dem Pfeil nach unten. Der ADK wird aktualisiert.

ADKs entfernen

So entfernen Sie einen ADK

1. Wählen Sie den ADK, den Sie entfernen möchten, in der Liste der ADKs aus. Der ausgewählte ADK wird markiert.
2. Klicken Sie auf das Minussymbol. In einer PGP-Warnung werden Sie aufgefordert, das Entfernen des ADK zu bestätigen.
3. Klicken Sie auf **OK**, um den ADK zu entfernen. Der ADK wird entfernt.

Mit Widerrufern arbeiten

Es kann vorkommen, dass Sie die Passphrase vergessen oder das Schlüsselpaar verlieren (falls beispielsweise Ihr Laptop gestohlen wird oder ein Festplattenfehler vorliegt).

Sofern Sie nicht die Schlüsselwiederherstellung verwenden, um den privaten Schlüssel wiederherzustellen, können Sie den Schlüssel nicht mehr verwenden und ihn auch nicht widerrufen, um anderen Personen anzuzeigen, dass er nicht mehr für die Verschlüsselung genutzt werden sollte. Als Schutzmaßnahme in derartigen Fällen können Sie eine Drittpartei als Schlüssel-Widerrufer einsetzen. Die von Ihnen eingesetzte Drittpartei kann den Schlüssel dann so widerrufen, als ob Sie ihn selbst widerrufen hätten.

Diese Funktion steht für Diffie-Hellman/DSS- und RSA-Schlüssel zur Verfügung.

Sie können nur die Widerrufer-Informationen Ihrer eigenen Schlüsselpaare ändern. Falls ein öffentlicher Schlüssel am Schlüsselbund einen Widerrufer aufweist, können Sie diese Informationen zwar einsehen, aber nicht ändern.

Designierte Widerrufer zu Schlüsseln hinzufügen

So fügen Sie einem Schlüssel einen designierten Widerrufer hinzu

1. Öffnen Sie PGP Desktop, klicken Sie auf das Bedienfeld „PGP Keys“ und dann auf **Eigene private Schlüssel**. Die privaten Schlüssel am Schlüsselbund werden angezeigt.
2. Doppelklicken Sie auf den Schlüssel, dem Sie einen Widerrufer hinzufügen möchten. Das Dialogfeld „Schlüsseleigenschaften“ für den von Ihnen ausgewählten Schlüssel wird angezeigt.
3. Klicken Sie falls erforderlich auf das Pluszeichen links neben **Widerrufer** (nur Schlüssel, denen bereits ein Widerrufer zugewiesen wurde, sind mit einem Pluszeichen gekennzeichnet). Die Widerrufer-Informationen für diesen Schlüssel werden angezeigt, falls konfiguriert.
4. Klicken Sie auf das Pluszeichen rechts neben dem Bereich „Widerrufer“. Das Dialogfeld „Schlüssel auswählen“ wird angezeigt.
5. Wählen Sie den Schlüssel aus, den Sie als Widerrufer-Schlüssel verwenden möchten, und klicken Sie auf **OK**.

   Sie werden in einem PGP-Warndialogfeld aufgefordert, das Hinzufügen der Widerrufer-Berechtigungen zu den ausgewählten Schlüsseln zu bestätigen.
6. Klicken Sie auf **Ja**, um fortzufahren, oder auf **Nein**, um abzubrechen. Das Dialogfeld „PGP-Passphrase für Schlüssel eingeben“ wird angezeigt.
7. Geben Sie die Passphrase für das Schlüsselpaar ein, dem Sie einen Widerrufer hinzufügen möchten, und klicken Sie auf **OK**.Das Dialogfeld „PGP-Informationen“ wird angezeigt.
8. Klicken Sie auf **OK**.Die ausgewählten Schlüssel sind jetzt zum Widerrufen des Schlüssels autorisiert. Zur effektiven Schlüsselverwaltung verteilen Sie eine aktuelle Kopie des Schlüssels an einen oder mehrere Widerrufer oder Sie laden den Schlüssel auf den Keyserver hoch.

Schlüssel widerrufen

Falls Sie Ihrem persönlichen Schlüsselpaar nicht mehr vertrauen sollten, können Sie den Schlüssel widerrufen. Dadurch teilen Sie allen Personen mit, dass sie Ihren öffentlichen Schlüssel nicht mehr verwenden sollten.

Sie können einen widerrufenen Schlüssel am besten verbreiten, indem Sie ihn auf einem öffentlichen Keyserver platzieren.

So widerrufen Sie einen Schlüssel

1. Öffnen Sie PGP Desktop, klicken Sie auf das Bedienfeld „PGP Keys“ und dann auf **Eigene private Schlüssel**. Die privaten Schlüssel am Schlüsselbund werden angezeigt.
2. Klicken Sie mit der rechten Maustaste auf den Schlüssel, den Sie widerrufen möchten, und wählen Sie dann aus der eingeblendeten Befehlsliste **Widerrufen** aus. Im Dialogfeld PGP-Warnung werden Sie aufgefordert, das Widerrufen des Schlüssels zu bestätigen.
3. Klicken Sie auf **Ja**, um das Widerrufen des ausgewählten Schlüssels zu bestätigen. Falls Sie den Vorgang abbrechen möchten, klicken Sie auf **Nein**. Das Dialogfeld „PGP-Passphrase für Schlüssel eingeben“ wird angezeigt.
4. Geben Sie die Passphrase für das Schlüsselpaar ein, das Sie widerrufen möchten, und klicken Sie auf **OK**.Ein widerrufener Schlüssel wird mit einem roten X gekennzeichnet, der angibt, dass der Schlüssel nicht mehr gültig ist.
5. Synchronisieren Sie den widerrufenen Schlüssel, damit alle Personen wissen, dass sie den nunmehr widerrufenen öffentlichen Schlüssel nicht mehr verwenden sollten.

Schlüssel teilen und wieder zusammenfügen

Mithilfe eines kryptografischen Vorgangs, der als Blakely-Shamir-Schlüsselteilung bekannt ist, können private Schlüssel auf mehrere Teilbesitzer aufgeteilt werden. Dieses Verfahren wird für Schlüssel mit extrem hohem Sicherheitsanspruch empfohlen.

Die PGP Corporation verwendet beispielsweise einen Unternehmensschlüssel, der auf mehrere Einzelpersonen aufgeteilt ist. Wenn der Schlüssel für die Signatur erforderlich ist, werden die Teile des Schlüssels vorübergehend wieder zusammengefügt.

Geteilte Schlüssel erstellen

Wenn Sie einen Schlüssel teilen, werden die Teile als Dateien gespeichert, die entweder an den öffentlichen Schlüssel eines Teilbesitzers verschlüsselt sind oder konventionell verschlüsselt sind, falls der Teilbesitzer nicht über einen öffentlichen Schlüssel verfügt. Nach der Schlüsselteilung wird bei jedem Signieren oder Entschlüsseln mit diesem Schlüssel automatisch versucht, den Schlüssel wieder zusammenzufügen.

So erstellen Sie einen Schlüssel mit mehreren Teilen

1. Öffnen Sie PGP Desktop, klicken Sie auf das Bedienfeld „PGP Keys“ und dann auf **Eigene private Schlüssel**. Die privaten Schlüssel am Schlüsselbund werden angezeigt.
2. Klicken Sie auf das Schlüsselpaar, das Sie teilen möchten. Das ausgewählte Schlüsselpaar wird hervorgehoben.
3. Klicken Sie auf **Schlüssel > Schlüssel teilen > Teilen**.Das Dialogfeld „Geteilter PGP-Schlüssel“ wird angezeigt.
4. Fügen Sie dem geteilten Schlüssel Teilbesitzer hinzu, indem Sie deren Schlüssel in die Liste **Teilbesitzer** ziehen und dort ablegen.

   Wenn Sie einen Teilbesitzer hinzufügen möchten, der nicht über einen öffentlichen Schlüssel verfügt, klicken Sie auf **Hinzufügen**, geben Sie den Namen der Person ein und lassen Sie die Person ihre Passphrase selbst eingeben. (Der Teilbesitzer muss physisch anwesend sein, um seine Passphrase eingeben zu können.)
5. Wenn alle Teilbesitzer aufgeführt sind, können Sie die Anzahl der Schlüsselteile angeben, die zum Entschlüsseln oder Signieren mit diesem Schlüssel erforderlich sein sollen.

   Standardmäßig ist jeder Teilbesitzer für einen Teil verantwortlich. Erhöhen Sie die Anzahl der Teile, die ein Teilbesitzer steuert, indem Sie auf den Namen in der Liste der Teilbesitzer klicken und mit den Pfeilen die Anzahl der Teile anpassen.
6. Klicken Sie auf **Schlüssel teilen**.Sie werden aufgefordert, ein Verzeichnis auszuwählen, in dem die Teile gespeichert werden sollen.
7. Wählen Sie einen Speicherort für die Schlüsselteile aus und klicken Sie auf **OK**.Der Passphrasen-Bildschirm wird angezeigt.
8. Geben Sie die Passphrase für den Schlüssel ein, den Sie teilen möchten, und klicken Sie auf **OK**. Ein Bestätigungsdialogfeld wird angezeigt.
9. Klicken Sie auf **Ja**, um den Schlüssel zu teilen. Der Schlüssel wird geteilt und die Teile werden am angegebenen Speicherort gespeichert. Die Schlüsselteile werden mit den Namen der Teilbesitzer als Dateinamen und mit der Dateiendung „.shf“ gespeichert.
10. Verteilen Sie die Schlüsselteile an die Besitzer und löschen Sie dann die lokalen Kopien der Teile.

    Nachdem ein Schlüssel auf mehrere Teilbesitzer aufgeteilt wurde, versucht PGP Desktop bei jedem Signieren oder Entschlüsseln mit diesem Schlüssel automatisch, den Schlüssel wieder zusammenzufügen.

Bewahren Sie den ursprünglichen Schlüssel, der geteilt wurde, sicher auf. Dieser Schlüssel ist erforderlich, um den geteilten Schlüssel für Entschlüsselungsfunktionen zusammenzufügen.

Geteilte Schlüssel wieder zusammenfügen

Nachdem ein Schlüssel auf mehrere Teilbesitzer aufgeteilt wurde, versucht PGP Desktop bei jedem Signieren oder Entschlüsseln mit diesem Schlüssel automatisch, den Schlüssel wieder zusammenzufügen. Es gibt zwei Möglichkeiten, den Schlüssel wieder zusammenzufügen: lokal und remote.

Beim lokalen Zusammenfügen von Schlüsselteilen muss der Teilbesitzer an dem Computer anwesend sein, an dem der Schlüssel zusammengefügt wird. Jeder Teilbesitzer muss die Passphrase für seinen Teil des Schlüssels eingeben.

Erfolgt das Zusammenfügen der Schlüsselteile remote, müssen die Remoteteilbesitzer ihre Schlüssel authentifizieren und entschlüsseln, bevor sie sie über das Netzwerk senden. Die TLS-Technologie (Transport Layer Security) von PGP Desktop stellt eine sichere Verbindung zum Übermitteln von Schlüsselteilen bereit, die es mehreren Einzelpersonen an räumlich getrennten Standorten ermöglicht, mit ihren Schlüsselteilen sicher zu signieren oder zu entschlüsseln.

Achtung: Bevor Schlüsselteile über das Netzwerk entgegengenommen werden, sollten Sie den Fingerabdruck jedes Teilbesitzers verifizieren und dessen öffentlichen Schlüssel signieren, um sicherzustellen, dass sein Authentifizierungsschlüssel legitim ist.

Vergewissern Sie sich bevor Sie beginnen, dass der ursprüngliche Schlüssel, der geteilt wurde, auf dem Computer vorhanden ist, an dem der Schlüssel zusammengefügt wird.

So fügen Sie einen geteilten Schlüssel wieder zusammen

1. Nehmen Sie mit jedem Teilbesitzer des geteilten Schlüssels Kontakt auf. Damit Schlüsselteile lokal zusammengefügt werden können, müssen die Teilbesitzer des Schlüssels anwesend sein.

   Damit Schlüsselteile über das Netzwerk gesammelt werden können, müssen Sie sicherstellen, dass die Remoteteilbesitzer PGP Desktop installiert haben und zum Senden ihrer Teiledatei des Schlüssel bereit sind. Die Remoteteilbesitzer benötigen Folgendes:

   - Ihre jeweiligen Schlüsselteildateien und Passphrasen
   - Ein Schlüsselpaar (zur Authentifizierung an dem Computer, der die Schlüsselteile sammelt)
   - Eine Netzwerkverbindung
   - Die IP-Adresse oder den voll qualifizierten Domänennamen des Computers, der die Schlüsselteile sammelt

2. Führen Sie einen der folgenden Schritte aus:

- Wenn Sie den Schlüssel vorübergehend wieder zusammenfügen möchten, wählen Sie an dem Computer, an dem der Schlüssel zusammengefügt wird, in Windows Explorer die Datei(en) aus, die Sie mit dem geteilten Schlüssel signieren oder entschlüsseln möchten.

  Klicken Sie mit der rechten Maustaste auf die Datei(en) und wählen Sie aus dem PGP-Kontextmenü die Option zum Signieren oder Entschlüsseln aus. Das Dialogfeld **PGP-Passphrase für ausgewählten Schlüssel eingeben** wird angezeigt, wobei der geteilte Schlüssel ausgewählt ist.

  Klicken Sie auf **OK**, um den ausgewählten Schlüssel neu zu erstellen. Das Dialogfeld „Schlüsselteilsammlung" wird angezeigt.

- Wenn der Schlüssel dauerhaft wieder zusammengefügt werden soll, klicken Sie mit der rechten Maustaste auf den geteilten Schlüssel und wählen Sie im angezeigten Menü die Option **Schlüsseleigenschaften** aus.

  Klicken Sie im Dialogfeld „Schlüsseleigenschaften" auf **Schlüssel zusammenfügen** (bei Schlüsseln, die nicht geteilt wurden, lautet die Bezeichnung der Schaltfläche **Passphrase ändern**).

Das Passphrasen-Dialogfeld wird angezeigt.

3 Führen Sie einen der folgenden Schritte aus:

- Falls Sie die Schlüsselteile lokal sammeln, klicken Sie auf **Teiledatei auswählen** und suchen Sie dann nach den Teiledateien, die dem geteilten Schlüssel zugeordnet sind. Die Teiledateien können von der Festplatte, einer Diskette oder einem aktivierten Laufwerk gesammelt werden. Fahren Sie mit dem nächsten Schritt fort.

- Falls Sie Schlüsselteile über das Netzwerk sammeln, klicken Sie auf **Netzwerk starten**. Der Remotebenutzer muss PGP Desktop aufrufen und auf **Schlüssel > Schlüssel teilen > Schlüsselteil senden** klicken. Dadurch kann die Teiledatei ausgewählt und entschlüsselt, der Autorisierungsschlüssel ausgewählt und entsperrt und der Hostname bzw. die IP-Adresse des Computers ausgewählt werden, der die Teile zusammenfügt.

  Wählen Sie im Feld „Signaturschlüssel" das Schlüsselpaar aus, das Sie zur Authentifizierung am Remotesystem verwenden möchten, und geben Sie die Passphrase ein.

  Klicken Sie auf **OK**, um den Computer auf den Empfang der Schlüsselteile vorzubereiten.

  Der Status der Transaktion wird im Feld „Netzwerkteile" angezeigt. Wenn sich der Status in „Abhören" ändert, ist die PGP-Anwendung zum Empfangen der Schlüsselteile bereit.

  Zu diesem Zeitpunkt müssen die Teilbesitzer ihre Schlüsselteile senden.

Wenn ein Schlüsselteil empfangen wird, wird das Dialogfeld „Remoteauthentifizierung“ angezeigt. Falls Sie den Schlüssel, der zur Authentifizierung des Remotesystems verwendet wird, nicht signiert haben, wird der Schlüssel als ungültig angesehen. Obwohl Sie den geteilten Schlüssel auch mit einem ungültigen Authentifizierungsschlüssel wieder zusammenfügen können, wird dieses Vorgehen nicht empfohlen. Sie sollten den Fingerabdruck jedes Teilbesitzers prüfen und dessen öffentlichen Schlüssel signieren, um sicherzustellen, dass der Authentifizierungsschlüssel legitim ist.

4. Klicken Sie auf **Bestätigen**, um die Teiledatei anzunehmen.
5. Sammeln Sie weiterhin Schlüsselteile, bis im Dialogfeld „Schlüsselteilsammlung“ die Werte für „Insgesamt gesammelte Teile“ und „Insgesamt erforderliche Teile“ übereinstimmen.
6. Klicken Sie auf **OK.**
   - Wenn der Schlüssel zum Entschlüsseln oder Signieren nur vorübergehend zusammengefügt wurde, wird die Datei mit dem geteilten Schlüssel signiert oder entschlüsselt. Danach wird der wieder zusammengefügte Schlüssel verworfen.
   - Wenn der Schlüssel dauerhaft zusammengefügt wurde, wird er als vollständig wieder zusammengefügter Schlüssel gespeichert (es handelt sich also nicht mehr um einen geteilten Schlüssel).

Vorgehensweise bei verloren gegangenen Schlüsseln oder Passphrasen

Wenn Sie Ihren Schlüssel verloren haben, können Sie ihn wiederherstellen, damit Sie weiterhin Daten verschlüsseln und entschlüsseln können. Die Vorgehensweise hierfür ist davon abhängig, ob Sie PGP Desktop als eigenständige Anwendung oder in einer von einem PGP Universal Server verwalteten Umgebung verwenden.

Wenn Sie die Passphrase vergessen haben, können Sie sie zurücksetzen. Dazu müssen Sie drei von fünf Sicherheitsfragen richtig beantworten, die Sie bei der Einrichtung des Schlüssels oder der Sicherheitsfragen beantwortet haben.

Schlüssel mit PGP Universal Server wiederherstellen

Dieser Abschnitt betrifft nur PGP Desktop-Benutzer in einer von einem PGP Universal Server verwalteten Umgebung, deren PGP-Administrator für die Installation von PGP Desktop eine Unterstützung zur Schlüsselwiederherstellung konfiguriert hat.

Falls Sie Ihren Schlüssel verlieren oder Ihre Passphrase vergessen und keine Sicherungskopie besitzen, von der Sie den Schlüssel wiederherstellen können, können Sie Informationen, die mit dem Schlüssel verschlüsselt wurden, nicht mehr entschlüsseln. Sie können den Schlüssel jedoch wiederherstellen, wenn der PGP-Administrator eine Richtlinie für die PGP-Schlüsselwiederherstellung für Sie implementiert hat. Dabei wird der Schlüssel verschlüsselt und so auf einem PGP Universal Server gespeichert, dass nur Sie ihn abrufen können.

Der PGP Universal Server, der die Schlüsselwiederherstellungsdaten besitzt, speichert Ihren Schlüssel so, dass nur Sie Zugriff auf ihn haben. Selbst der PGP-Administrator kann Ihren Schlüssel nicht entschlüsseln.

Falls der PGP-Administrator die Unterstützung für die Schlüsselwiederherstellung konfiguriert hat, werden Sie bei der Installation von PGP Desktop oder beim Erstellen von Sicherheitsfragen aufgefordert, zusätzliche „geheime“ Informationen einzugeben.

Sobald sich der Schlüssel auf dem Server befindet, können Sie ihn jederzeit wiederherstellen, indem Sie in PGP Desktop für Windows auf **Schlüssel > Ich habe meinen Schlüssel verloren** bzw. auf **Schlüssel > Ich habe meine Passphrase vergessen** oder in PGP Desktop für Mac OS X auf **Schlüssel > Wiederherstellen** klicken.

Tipp: Wenn Sie während der Installation von PGP Desktop nicht aufgefordert wurden, Ihre PGP-Fragen zu erstellen, und der PGP Universal Server-Administrator die lokale Schlüsselwiederherstellung zulässt, können Sie die Fragen manuell erstellen. Weitere Informationen finden Sie unter *Sicherheitsfragen erstellen* (auf Seite 91).

Schlüsselwiederherstellungsdaten erstellen

Beim Beantworten der PGP-Sicherheitsfragen erstellen Sie die Schlüsselwiederherstellungsdaten. In einer eigenständigen Umgebung werden diese Informationen auf der lokalen Festplatte in einer KRB-Datei gespeichert. In einer verwalteten Umgebung werden die Schlüsselwiederherstellungsdaten an den PGP Universal Server des Unternehmens gesendet, wenn Sie PGP Desktop installieren oder wenn Sie Sicherheitsfragen erstellen und beantworten.

Wählen Sie geheime persönliche Fragen mit Antworten aus, die Sie nicht vergessen werden. Die Fragen können bis zu 95 Zeichen umfassen. Eine gute Frage ist beispielsweise „Mit wem bin ich zum Strand gegangen?“ oder „Warum ist Fred weggegangen?“. Eine schlechte Frage wäre beispielsweise „Wie lautet der Mädchenname meiner Mutter?“ oder „Auf welches Gymnasium bin ich gegangen“.

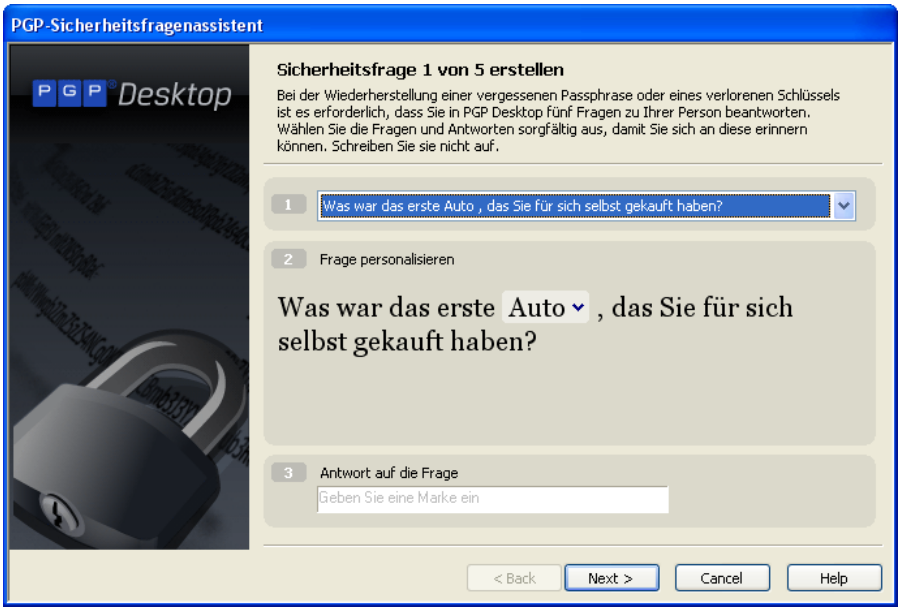
Wenn Sie alle fünf PGP-Fragen erstellt und beantwortet haben, wird Ihr privater Schlüssel mithilfe der Blakely-Shamir-Schlüsselteilung in fünf Teile geteilt. Drei der fünf Teile sind für die Wiederherstellung des Schlüssels erforderlich. Die Teile werden dann mit dem Hash, der eindeutigen Identifizierungsnummer einer Antwort, verschlüsselt. Wenn Sie drei beliebige Antworten kennen, können Sie den gesamten Schlüssel erfolgreich wiederherstellen.

Sicherheitsfragen erstellen

Bevor Sie einen Schlüssel wiederherstellen oder eine neue Passphrase erstellen können, wenn Sie die alte vergessen haben, müssen Sie Sicherheitsfragen erstellen. Sie können die fünf Sicherheitsfragen anpassen, damit die Antworten ausschließlich Ihnen bekannt sind.

So erstellen Sie Sicherheitsfragen

1. Klicken Sie in PGP Desktop auf das Bedienfeld „PGP Keys“ und wählen Sie Ihren Schlüssel aus.
2. Klicken Sie auf **Schlüssel > PGP-Fragen erstellen**. Der PGP-Sicherheitsfragenassistent wird angezeigt.
3. Geben Sie die Passphrase des Schlüssels ein und klicken Sie auf **Weiter**. Das Dialogfeld „Sicherheitsfrage 1 von 5 erstellen“ wird angezeigt.


PGP-Sicherheitsfragenassistent
PGP Desktop
Sicherheitsfrage 1 von 5 erstellen
Bei der Wiederherstellung einer vergessenen Passphrase oder eines verlorenen Schlüssels ist es erforderlich, dass Sie in PGP Desktop fünf Fragen zu Ihrer Person beantworten. Wählen Sie die Fragen und Antworten sorgfältig aus, damit Sie sich an diese erinnern können. Schreiben Sie sie nicht auf.
1
Was war das erste Auto , das Sie für sich selbst gekauft haben?
2
Frage personalisieren
Was war das erste Auto , das Sie für sich selbst gekauft haben?
3
Antwort auf die Frage
Geben Sie eine Marke ein
< Back
Next >
Cancel
Help

4. Klicken Sie im ersten Dialogfeld zum Erstellen der Sicherheitsfragen auf den Pfeil für das erste Feld, um die Frage auszuwählen, die Sie verwenden möchten. Beachten Sie, dass Sie Teile der Frage im nächsten Schritt anpassen können.

   Wenn Sie eine Frage eigenständig definieren möchten, klicken Sie auf **Geben Sie Ihre eigene Frage ein**.
5. Klicken Sie für die Option **Frage personalisieren** auf die Pfeile neben dem anpassbaren Text. Wenn Sie beispielsweise die erste Frage ausgewählt haben, können Sie die Frage anpassen, indem Sie „erste“ durch „zweite“ und „in die Sie verliebt waren“ durch „mit der Sie Händchen gehalten haben“ ersetzen.

Wenn Sie eine eigene Frage erstellen, geben Sie die Frage in diesem Feld ein. Geben Sie eine Frage ein, auf die nur Sie die Antwort kennen.

6 Geben Sie unter **Antwort auf die Frage** die Antwort auf diese Sicherheitsfrage ein. Sie können die Antwort unter Beachtung von Groß- und Kleinschreibung eingeben. Wenn Sie die Frage beantworten, spielt diese jedoch keine Rolle.

In diesem Feld wird ein Hinweis angezeigt, der ausgeblendet wird, sobald Sie mit der Eingabe der Antwort beginnen. Beispielweise wird für die Antwort auf die Frage „Wie hieß die erste Person, mit der Sie Händchen gehalten haben" der Hinweis „Geben Sie den Vor- und Nachnamen ein" angezeigt.

7 Wenn Sie die Frage festgelegt und die Antwort eingegeben haben, klicken Sie auf **Weiter**, um fortzufahren. Das Dialogfeld „Sicherheitsfrage 2 von 5 erstellen" wird angezeigt.

8 Sie werden insgesamt zur Eingabe und Beantwortung von fünf Sicherheitsfragen aufgefordert. Wiederholen Sie die oben genannten Schritte, um eine Frage auszuwählen, anzupassen und zu beantworten.

Wenn Sie alle fünf Fragen und Antworten eingegeben haben, wird das Dialogfeld „PGP-Sicherheitsfragenassistent wird abgeschlossen" angezeigt. Klicken Sie auf **Fertig stellen**, um den Assistenten zu beenden.

Sie haben jetzt die fünf Sicherheitsfragen festgelegt. Wenn Sie Ihren Schlüssel verloren oder Ihre Passphrase vergessen haben, können Sie den Schlüssel wiederherstellen oder die Passphrase zurücksetzen, indem Sie mindestens drei der fünf Sicherheitsfragen richtig beantworten.

Schlüssel bei verloren gegangenen Schlüsseln bzw. Passphrasen wiederherstellen

Wenn Sie Ihren Schlüssel verloren oder die Passphrase vergessen haben, ist eine Wiederherstellung möglich, indem Sie den Schlüssel wiederherstellen. Dazu müssen Sie Sicherheitsfragen erstellt haben, die nur Sie beantworten können. Weitere Informationen finden Sie unter *Sicherheitsfragen erstellen* (auf Seite 91).

So stellen Sie Ihren Schlüssel wieder her

1 Klicken Sie in PGP Desktop auf das Bedienfeld „PGP Keys" und wählen Sie Ihren Schlüssel aus.

2 Klicken Sie auf **Schlüssel > Ich habe meinen Schlüssel verloren**. Das Dialogfeld Assistent für PGP-Passphrasen: Sicherheitsfragen beantworten wird angezeigt.

Assistent für PGP-Passphrasen
PGP Desktop
Sicherheitsfragen beantworten
Dies sind die benutzerdefinierten Fragen, die Sie beim Erstellen der Passphrase erstellt haben. Sie müssen mindestens drei richtige Antworten geben.
Wie hieß die zweite Person, in die Sie verliebt waren ?
1
Geben Sie den Vor- und Nachnamen ein
Was war Ihre zweite Wahl für den Namen Ihres/Ihrer Katze ?
2
Geben Sie den Namen ein
Was war Ihr Lieblingsmuseum im Sommerurlaub ?
3
Geben Sie einen Urlaubsort ein
Wer/welche/welcher war der/die Ihnen am unsympathischste Bas...
4
Geben Sie den vollständigen Namen ein
Geben Sie eine Musikgruppe ein, das/die/der Erinnerungen an Ihr...
5
Geben Sie den vollständigen Namen ein
Dies sind nicht meine Fragen.
< Back
Next >
Cancel
Help

Tipp: Wenn es sich bei den angezeigten Fragen nicht um Ihre eigenen Fragen handelt, klicken Sie auf den Link „Dies sind nicht meine Fragen“. Das Dialogfeld Assistent für PGP-Passphrasen: Wiederherzustellenden Schlüssel auswählen wird angezeigt. Wählen Sie die Schlüssel-ID des Schlüssels aus, den Sie wiederherstellen möchten, und klicken Sie auf **Weiter**.

3 Beantworten Sie drei der fünf Sicherheitsfragen richtig und klicken Sie auf **Weiter**. Das Dialogfeld „Assistent für PGP-Passphrasen: Erfolg“ wird angezeigt.

4 Klicken Sie auf **Weiter**, um mit der Erstellung einer neuen Passphrase fortzufahren. Das Dialogfeld Assistent für PGP-Passphrasen: Passphrase erstellen wird angezeigt.

5 Geben Sie die Passphrase zwei Mal ein.

Wenn die Zeichen während der Eingabe der Passphrase angezeigt werden sollen, aktivieren Sie das Kontrollkästchen **Tastatureingabe anzeigen**. Stellen Sie sicher, dass niemand sehen kann, was Sie eingeben.

Die Passphrasen-Qualitätsanzeige gibt Ihnen eine Richtlinie für die Stärke der Passphrase, die Sie erstellen. Sie vergleicht den Entropiewert der eingegebenen Passphrase mit einer echten zufälligen Zeichenkette mit 128 Bit (der gleiche Entropiewert wie in einem AES128-Schlüssel). Weitere Informationen finden Sie unter *Passphrasen-Qualitätsanzeige* (siehe "Die Passphrasen-Qualitätsanzeige" auf Seite 352).

6 Klicken Sie auf **Beenden**. Der Schlüssel wurde wiederhergestellt.

Schlüssel schützen

Sie sollten nicht nur Sicherungskopien Ihrer Schlüssel erstellen, sondern auch besonders sorgsam darauf achten, wo Sie den privaten Schlüssel aufbewahren. Obwohl der private Schlüssel durch eine Passphrase geschützt ist, die nur Sie kennen sollten, ist es möglich, dass eine andere Person Ihre Passphrase in Erfahrung bringt und Ihren privaten Schlüssel zum Entschlüsseln von E-Mail-Nachrichten oder zum Fälschen Ihrer digitalen Signatur verwendet. Jemand könnte Ihnen beispielsweise über die Schulter blicken und beobachten, welche Tastatureingaben Sie vornehmen, oder die Tastatureingaben über das Netzwerk oder sogar über das Internet abfangen.

Damit andere Personen, die Ihre Passphrase abgefangen haben, Ihren privaten Schlüssel nicht nutzen können, sollten Sie diesen ausschließlich auf Ihrem eigenen Computer speichern. Falls der Computer mit einem Netzwerk verbunden ist, stellen Sie sicher, dass Ihre Dateien nicht automatisch in eine systemweite Sicherung einbezogen werden, über die andere Personen Zugriff auf Ihren privaten Schlüssel erhalten könnten. Da ein Zugriff auf Computer in einem Netzwerk recht problemlos möglich ist, sollten Sie Ihren privaten Schlüssel auf einem Flash-Laufwerk speichern, falls Sie mit extrem vertraulichen Daten arbeiten. Dieses Laufwerk kann wie ein traditioneller Schlüssel immer dann angeschlossen werden, wenn Sie private Informationen lesen oder signieren möchten.

Als weitere Sicherheitsmaßnahme könnten Sie Ihrer privaten Schlüsselbunddatei einen anderen Namen zuweisen und sie nicht am Standardspeicherort speichern.

Ihre privaten und öffentlichen Schlüssel werden in getrennten Schlüsselbunddateien gespeichert. Sie können sie an einen anderen Speicherplatz auf der Festplatte oder auf einer Diskette kopieren. Standardmäßig werden der private Schlüsselbund (`secring.skr`) und der öffentliche Schlüsselbund (`pubring.pkr`) zusammen mit anderen Programmdateien im PGP-Ordner gespeichert. Sicherungskopien können an einem beliebigen Speicherort gespeichert werden.

Sie können PGP Desktop so konfigurieren, dass Schlüsselbunde automatisch nach dem Beenden von >prod< gesichert werden. Legen Sie die Sicherungsoptionen für Schlüsselbunde im Dialogfeld „Optionen“ auf der Registerkarte „Schlüssel“ (Windows) bzw. im Dialogfeld „Einstellungen“ (Mac OS X) fest.

Tipp: Wenn Sie die Passphrase des Schlüssels ändern, wird die Passphrase von Kopien des Schlüssels (z. B. Sicherungskopien) nicht geändert. Wenn Sie annehmen, dass die Passphrase nicht mehr geheim ist, empfiehlt die PGP Corporation, alle Sicherungskopien sicher zu löschen und neue Sicherungskopien des Schlüssels zu erstellen.

7 E-Mail-Nachrichten sichern

In diesem Abschnitt wird beschrieben, wie Sie E-Mail-Nachrichten automatisch und transparent mit PGP Desktop Email sichern.

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung verwenden, hat Ihr PGP Universal Server-Administrator ggf. bestimmte Funktionen deaktiviert. Ist eine Funktion deaktiviert, wird das Bedienelement auf der linken Seite nicht angezeigt und das Menü oder andere auf diese Funktion zutreffenden Optionen sind nicht verfügbar. Die in diesem Handbuch enthaltenen Abbildungen entsprechen der Standardinstallation, bei der alle Funktionen aktiviert sind. Wenn Ihr PGP Universal Server-Administrator diese Funktion deaktiviert hat, ist dieser Abschnitt für Sie nicht relevant.

In diesem Kapitel

E-Mail-Nachrichten mit PGP Desktop sichern 95
Offline-Richtlinien verwenden 101
Dienste und Richtlinien 103
Neue Sicherheitsrichtlinien erstellen 114
Mit der Sicherheitsrichtlinienliste arbeiten 127
PGP Desktop und SSL 134
Schlüsselmodi 136
PGP-Protokoll anzeigen 140

E-Mail-Nachrichten mit PGP Desktop sichern

Wenn der Schutz von E-Mail-Nachrichten aktiviert ist, überwacht PGP Desktop den E-Mail-Verkehr zwischen dem E-Mail-Client und dem E-Mail-Server. PGP Desktop schaltet sich je nach Bedarf zu, um Nachrichten zu verschlüsseln, zu signieren, zu entschlüsseln oder zu verifizieren.

Nach der ordnungsgemäßen Konfiguration, die in der Regel von PGP Desktop automatisch durchgeführt wird, ist kein Eingriff Ihrerseits erforderlich, um ausgehende Nachrichten zu verschlüsseln und/oder zu signieren bzw. eingehende Nachrichten zu entschlüsseln und/oder zu verifizieren. Der Messaging-Proxy von PGP Desktop übernimmt diese Aufgaben für Sie.

Der Ablauf dieser Prozesse ist für eingehende und ausgehende Nachrichten unterschiedlich.

PGP Desktop überprüft automatisch alle eingehenden E-Mail-Nachrichten und führt die entsprechenden Aktionen aus (wie im folgenden Abschnitt beschrieben).

Bei ausgehenden Nachrichten kann PGP Desktop auf Basis der konfigurierten Richtlinien verschiedene Aktionen für Sie ausführen. Eine Richtlinie ist ein Satz von Anweisungen (z. B. „Wenn dies passiert, folgende Aktion durchführen"), mit denen PGP Desktop vorgeschrieben wird, wie in bestimmten Situationen vorzugehen ist. Durch die Kombination dieser Anweisungen lassen sich maßgeschneiderte Richtlinien für Ihre Anforderungen an die E-Mail-Sicherheit erstellen. PGP Desktop wird mit einem Satz vorkonfigurierter Richtlinien ausgeliefert, die dem Bedarf der meisten Benutzer gerecht werden. Dennoch behalten Sie die Kontrolle über alle Details dieser Richtlinien, falls Sie Änderungswünsche haben.

Wenn Sie PGP Desktop als eigenständige Lösung einsetzen und eine Nachricht senden, sucht PGP Desktop standardmäßig nach einem vertrauenswürdigen Schlüssel zum Verschlüsseln der Nachricht. Zunächst wird der Standardschlüsselring (unter Windows als „Alle Schlüssel" bezeichnet) oder der lokale Schlüsselbund (unter Mac OS X als „Schlüssel" bezeichnet) nach dem öffentlichen Schlüssel des Empfängers durchsucht. Wird der Schlüssel dort nicht gefunden, wird standardmäßig im PGP Global Directory nach einem vertrauenswürdigen Schlüssel für den Empfänger gesucht. Wenn dort kein vertrauenswürdiger Schlüssel zu finden ist, wird die Nachricht als Klartext gesendet, d. h. unverschlüsselt. Dieses standardmäßige Verhalten wird als *opportunistische Verschlüsselung* bezeichnet. Dabei handelt es sich um einen Kompromiss zwischen dem Schutz ausgehender Nachrichten und der Gewährleistung, dass die Nachrichten gesendet werden.

Informationen zum Erstellen neuer Richtlinien finden Sie unter *Neue Sicherheitsrichtlinien erstellen* (auf Seite 114).

Wenn Sie in einer mit PGP Universal geschützten Domäne arbeiten, bestimmen die lokalen PGP Desktop-Richtlinien, wie und wann Ihre Nachrichten verschlüsselt werden. Weitere Informationen erhalten Sie vom PGP Universal Server-Administrator Ihrer Organisation.

Hinweis: PGP Desktop überprüft nur den Standardschlüsselbund. Wenn Sie eine verschlüsselte E-Mail-Nachricht an einen Empfänger senden möchten, dessen Schlüssel sich am lokalen Schlüsselbund befindet, müssen Sie den Schlüssel an den Standardschlüsselbund importieren.

Wenn Sie über mehrere Schlüsselbunde verfügen, wird der Standardschlüsselbund im Bedienfeld „PGP Keys" an erster Stelle aufgeführt. Sie können einen anderen Schlüsselbund als Standardschlüsselbund festlegen, indem Sie im Bedienfeld „PGP Keys" mit der rechten Maustaste auf den Schlüsselbund klicken. Wählen Sie „Eigenschaften" aus und aktivieren Sie das Kontrollkästchen **Standardschlüsselbund**.

Eingehende Nachrichten

PGP Desktop entscheidet anhand des Nachrichteninhalts, wie mit einer eingehenden E-Mail-Nachricht vorgegangen wird. **Bei den folgenden Szenarien wird davon ausgegangen, dass PGP Desktop als eigenständige Lösung eingesetzt wird und nicht in einer von einen PGP Universal Server geschützten Domäne installiert ist** (bei einem PGP Universal Server werden u. U. E-Mail-Richtlinien angewendet, die vom PGP Universal Server-Administrator festgelegt wurden):

- **Die Nachricht ist weder verschlüsselt noch signiert.** Derartige Nachrichten werden von PGP Desktop ohne Überprüfung ihres Inhalts an den E-Mail-Client weitergeleitet.
- **Die Nachricht ist verschlüsselt, jedoch nicht signiert.** Wenn eine verschlüsselte Nachricht eingeht, versucht PGP Desktop, die Nachricht zu entschlüsseln. Zu diesem Zweck durchsucht PGP Desktop den lokalen Schlüsselbund nach dem privaten Schlüssel, mit dem die Nachricht entschlüsselt werden kann. Falls sich der private Schlüssel nicht am lokalen Schlüsselbund befindet, kann PGP Desktop die Nachricht nicht entschlüsseln und übergibt sie verschlüsselt an den E-Mail-Client. Ist der private Schlüssel am lokalen Schlüsselbund **vorhanden und die Passphrase ist für den privaten Schlüssel zwischengespeichert, wird die Nachricht sofort von PGP Desktop entschlüsselt. Ist die Passphrase nicht zwischengespeichert, werden Sie von PGP Desktop zur Eingabe der Passphrase aufgefordert. Sobald Sie die richtige Passphrase eingegeben haben, wird die Nachricht entschlüsselt. Nach dem Entschlüsseln der Nachricht übergibt PGP Desktop diese an den E-Mail-Client.**

  Wenn der Messaging-Proxy von PGP Desktop deaktiviert ist, kann PGP Desktop eingehende verschlüsselte Nachrichten nicht entschlüsseln. Die Nachrichten werden dann verschlüsselt an den E-Mail-Client weitergeleitet. Wenn Sie voraussichtlich verschlüsselte Nachrichten senden und empfangen werden, sollten Sie den Messaging-Proxy ständig aktiviert lassen. Der Proxy ist standardmäßig aktiviert.

- **Die Nachricht ist signiert, jedoch nicht verschlüsselt.** PGP Desktop durchsucht den lokalen Schlüsselbund nach einem öffentlichen Schlüssel, der zum Verifizieren der Signatur verwendet werden kann. Falls PGP Desktop den entsprechenden öffentlichen Schlüssel nicht am lokalen Schlüsselbund finden kann, sucht die Anwendung zunächst nach einem Keyserver unter „keys.domain“ (wobei **domain** die Domäne des Nachrichtenabsenders bezeichnet), dann im *PGP Global Directory* (https://keyserver.pgp.com) und schließlich auf anderen konfigurierten Keyservern. Wenn PGP Desktop den richtigen öffentlichen Schlüssel an einem dieser Speicherorte findet, wird die Signatur verifiziert (bzw. nicht verifiziert, falls sie ungültig ist). Dann wird die Nachricht mit einer Anmerkung zur Signatur an den E-Mail-Client weitergeleitet. Die entsprechenden Angaben werden außerdem im PGP-Protokoll vermerkt. Kann PGP Desktop den entsprechenden öffentlichen Schlüssel nicht finden, wird die Nachricht ohne Verifizierung an den E-Mail-Client weitergeleitet.
- **Die Nachricht ist verschlüsselt und signiert.** PGP Desktop führt beide der oben beschriebenen Verfahren durch: Zunächst wird der private Schlüssel zum Entschlüsseln der Nachricht gesucht, dann der öffentliche Schlüssel zum Verifizieren der Signatur. Sollte eine Nachricht jedoch nicht entschlüsselt werden können, kann sie auch nicht verifiziert werden.

Falls PGP Desktop eine Nachricht weder entschlüsseln noch verifizieren kann, sollten Sie sich eventuell mit dem Absender der Nachricht in Verbindung setzen. Konnte die Nachricht nicht entschlüsselt werden, vergewissern Sie sich, dass der Absender Ihren echten öffentlichen Schlüssel verwendet hat. Falls die Nachricht nicht verifiziert werden konnte, bitten Sie den Absender, seinen Schlüssel im PGP Global Directory zu veröffentlichen. Ältere PGP-Versionen und andere OpenPGP-Produkte können auf die Webversion dieses Verzeichnisses unter *PGP Global Directory* (https://keyserver.pgp.com) zugreifen. Sie können den Absender auch bitten, seinen öffentlichen Schlüssel per E-Mail an Sie zu senden.

Hinweis: PGP Desktop verschlüsselt standardmäßig nur an Schlüssel, die als gültig bekannt sind. Wenn Sie keinen Schlüssel vom PGP Global Directory erhalten haben, müssen Sie u. U. den Fingerabdruck des Schlüssels mit dem Besitzer abgleichen und ihn signieren, damit Sie ihn verwenden können.

Ausgehende Nachrichten

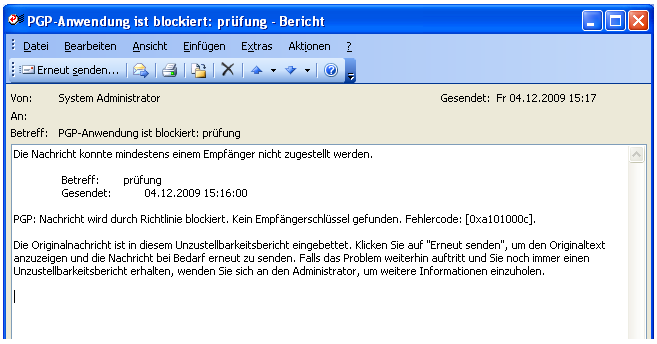
Von Ihnen gesendete E-Mail-Nachrichten können verschlüsselt, signiert, verschlüsselt und signiert oder weder verschlüsselt noch signiert sein. Da Sie wahrscheinlich unterschiedliche Kombinationen für verschiedene Empfänger oder E-Mail-Domänen benötigen, müssen Sie für ausgehende E-Mail-Nachrichten Richtlinien für alle Möglichkeiten erstellen. Nachdem die gewünschten Richtlinien festgelegt wurden, werden Ihre E-Mail-Nachrichten automatisch und transparent geschützt.

Wenn Sie in einer von einem PGP Universal Server verwalteten Umgebung arbeiten, werden Ihre PGP Desktop-Richtlinien durch die vom PGP Universal Server-Administrator festgelegten Richtlinien gesteuert. Möglicherweise hat der Administrator auch festgelegt, wie ausgehende E-Mail-Nachrichten gehandhabt werden sollen, wenn der PGP Universal Server nicht verfügbar ist. Diese Richtlinien werden als Offline-Richtlinien oder lokale Richtlinien bezeichnet.

MAPI-E-Mail-Nachrichten mit Microsoft Outlook senden

Eine neue Funktion in PGP Desktop Version 9.10 ist die Möglichkeit, ausgehende Nachrichten in eine Warteschlange einzureihen, damit Sie weiterhin im E-Mail-Programm arbeiten können und nicht darauf warten müssen, dass die PGP Notifier-Meldung ausgeblendet wird.

Wenn ein Schlüssel nicht gefunden wird, wird nicht die PGP Notifier-Meldung und dann die ausgehende Nachricht angezeigt (damit Sie diese ändern können, um beispielsweise den Empfänger zu ändern), stattdessen wird ein Unzustellbarkeitsbericht „Schlüssel nicht gefunden“ erstellt und gesendet. Der Bericht hat das Format einer eingehenden E-Mail-Nachricht und zeigt als Absender den Systemadministrator an. Er enthält Informationen dazu, warum die E-Mail-Nachricht einigen oder allen Empfängern nicht zugestellt werden konnte.


PGP-Anwendung ist blockiert: prüfung - Bericht
Datei Bearbeiten Ansicht Einfügen Extras Aktionen ?
Erneut senden...
Von: System Administrator
Gesendet: Fr 04.12.2009 15:17
An:
Betreff: PGP-Anwendung ist blockiert: prüfung
Die Nachricht konnte mindestens einem Empfänger nicht zugestellt werden.
Betreff: prüfung
Gesendet: 04.12.2009 15:16:00
PGP: Nachricht wird durch Richtlinie blockiert. Kein Empfängerschlüssel gefunden. Fehlercode: [0xa101000c].
Die Originalnachricht ist in diesem Unzustellbarkeitsbericht eingebettet. Klicken Sie auf "Erneut senden", um den Originaltext anzuzeigen und die Nachricht bei Bedarf erneut zu senden. Falls das Problem weiterhin auftritt und Sie noch immer einen Unzustellbarkeitsbericht erhalten, wenden Sie sich an den Administrator, um weitere Informationen einzuholen.

Folgende Nachrichten werden am häufigsten in einem Unzustellbarkeitsbericht aufgeführt:

- PGP: Nachricht wird durch Richtlinie blockiert. Server ist nicht erreichbar.
- PGP: Nachricht wird blockiert. Additional Decryption Key (ADK) wurde nicht gefunden.
- PGP: Nachricht wird blockiert. Signaturschlüssel konnte nicht entsperrt werden.
- PGP: Nachricht wird blockiert. Schlüssel wurde anhand der Schlüssel-ID nicht gefunden.
- PGP: Nachricht wird blockiert. Blockierung durch Notifier.
- PGP: Nachricht wird durch Richtlinie blockiert. Kein Empfängerschlüssel gefunden.
- PGP: Nachricht wird durch Richtlinie blockiert.

Wenden Sie sich bei Problemen mit Richtlinien an den PGP Universal Server-Administrator.

Signier- und Verschlüsselungsschaltflächen in Microsoft Outlook verwenden

In PGP Desktop für Windows 10.0 ist eine neue Funktion für Microsoft Outlook 2002 SP3, 2003 (XP) SP3 und 2007 bei gemeinsamer Verwendung mit Microsoft Exchange (MAPI)- und SMTP-E-Mail-Konten verfügbar. Diese neue Funktion bietet Schaltflächen zum expliziten Signieren, Verschlüsseln oder zum Signieren und Verschlüsseln von E-Mail-Nachrichten. Sie dient zur Einhaltung von Signaturvorschriften (z. B. der EU), die erfordern, dass Benutzer E-Mail-Nachrichten bewusst signieren.

Die Schaltflächen **Signieren** und **Verschlüsseln** sind sowohl für verwaltete als auch für eigenständige Installationen von PGP Desktop verfügbar.

- In eigenständigen Umgebungen werden die Schaltflächen zum Signieren und Verschlüsseln im Dialogfeld „Optionen“ aktiviert bzw. deaktiviert. Klicken Sie hierzu auf **Extras > Optionen**, wählen Sie die Registerkarte „Messaging“ aus und aktivieren (bzw. deaktivieren) Sie die Option **PGP-Verschlüsselungs- und Signierschaltflächen in Outlook aktivieren**. Die Schaltflächen sind standardmäßig deaktiviert.
- Wenn Sie PGP Desktop in einer verwalteten Umgebung einsetzen, hat der PGP Universal Server-Administrator festgelegt, ob diese Funktion verfügbar ist, oder er hat diese Funktion per Richtlinie deaktiviert.

Bei Aktivierung in Microsoft Outlook 2002/2003 werden beide Schaltflächen in der Symbolleiste angezeigt:

Bei Aktivierung in Microsoft Outlook 2007 werden beide Schaltflächen in der Nachrichtenleiste angezeigt:

Die Richtlinie für ausgehende E-Mail-Nachrichten bestimmt, wie die E-Mail-Nachricht gesendet wird. Neue Installationen von PGP Desktop enthalten drei neue Standardrichtlinien zur Unterstützung dieser Schaltflächen. Für bestehende Installationen müssen diese drei Standardrichtlinien erstellt werden. Weitere Informationen zu den Einstellungen für die Richtlinien finden Sie unter *Informationen und Beispiele zu Sicherheitsrichtlinien* (auf Seite 122).

Die Schaltflächen **Signieren** und **Verschlüsseln** stellen eine zusätzliche Funktion dar, mit der Sie steuern können, welche E-Mail-Nachrichten verschlüsselt und/oder signiert werden müssen. Die Schaltflächen dienen nicht als Ersatz für die in PGP Desktop verwendete E-Mail-Proxyfunktion.

Hinweis: Wenn Sie eine E-Mail-Nachricht beantworten oder weiterleiten und diese Nachricht verschlüsseln und/oder signieren möchten, müssen Sie die entsprechenden Schaltflächen auswählen. Weitergeleitete E-Mail-Nachrichten oder Antworten werden als neue Nachrichten behandelt, sodass Sie explizit die Optionen zum Sichern der Nachricht auswählen müssen.

Gehen Sie sowohl beim Erstellen neuer E-Mail-Nachrichten als auch beim Weiterleiten oder Beantworten von E-Mail-Nachrichten folgendermaßen vor.

So signieren, verschlüsseln oder signieren und verschlüsseln Sie eine E-Mail-Nachricht

1. Erstellen Sie eine E-Mail-Nachricht.
2. Führen Sie einen der folgenden Schritte aus:
   - Wenn Sie die Nachricht nur signieren möchten, klicken Sie auf **Signieren** (). Wenn Sie nur signieren möchten, wird die E-Mail-Nachricht als Klartext gesendet.
   - Wenn Sie die Nachricht nur verschlüsseln möchten, klicken Sie auf **Verschlüsseln** ().
   - Wenn Sie die Nachricht signieren *und* verschlüsseln möchten, klicken Sie sowohl auf **Signieren** als auch auf **Verschlüsseln** ().

   Tipp: Wenn Sie eine oder beide Schaltflächen ausgewählt haben und die E-Mail-Nachricht dann als Entwurf speichern, bleiben die Schaltflächen aktiviert, wenn Sie die Nachricht weiter verfassen.
3. Verfassen Sie die E-Mail-Nachricht weiter und senden Sie sie. Der Notifier von PGP Desktop zeigt das Ergebnis des Signier- und/oder Verschlüsselungsvorgangs an (weitere Informationen zu Benachrichtigungen finden Sie unter *PGP Desktop Notifier-Meldungen zu ausgehenden Nachrichten* (auf Seite 37)).

Offline-Richtlinien verwenden

Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, wird die Offline-Richtlinie für E-Mail-Nachrichten vom PGP Universal Server-Administrator festgelegt. Diese Richtlinie gibt an, wie E-Mail-Nachrichten gehandhabt werden, wenn der PGP Universal Server offline ist oder von PGP Desktop nicht erreicht werden kann.

- **Ausgehende Nachricht blockieren**: Ausgehende Nachrichten werden nicht gesendet. Wenn die Nachrichten vom E-Mail-Client in der Warteschlange gespeichert werden können, verbleiben sie in der Warteschlange, bis der PGP Universal Server verfügbar ist. Wenn die Nachrichten nicht in der Warteschlange gespeichert werden können, werden die E-Mail-Nachrichten blockiert.
- **Ausgehende Nachrichten als Klartext senden**: Sie werden gefragt, ob Sie die E-Mail-Nachricht ungesichert senden möchten. Wenn Sie die Nachricht senden möchten, wird sie als Klartext gesendet. Wenn Sie sie nicht senden möchten, wird die Nachricht blockiert.
- **Eigenständige Richtlinie befolgen**: PGP Desktop befolgt die eigenständige Richtlinie zur Verarbeitung Ihrer ausgehenden Nachrichten. Weitere Informationen finden Sie unter *Dienste und Richtlinien anzeigen* (auf Seite 104).

Weitere Informationen zu den Notifier-Meldungen, die Sie in den oben beschriebenen Fällen erhalten, finden Sie unter *PGP Desktop Notifier-Meldungen zu ausgehenden Nachrichten für Offline-Richtlinien* (auf Seite 38).

Der PGP Universal Server-Administrator kann festlegen, wie oft Ihre E-Mail-Richtlinien in PGP Desktop heruntergeladen werden. Wenn Sie sich im Offlinemodus befinden, bleibt die letzte heruntergeladene Offline-E-Mail-Richtlinie für die Verarbeitung der ausgehenden E-Mail-Nachrichten in Kraft. Wenn Sie sich für einen Zeitraum im Offlinemodus befinden, der länger ist als die für die Gültigkeit der eigenständigen Offline-E-Mail-Richtlinie zulässige Frist, hat der Administrator möglicherweise auch festgelegt, wie ausgehende E-Mail-Nachrichten verarbeitet werden sollen. In diesem Fall kann PGP Desktop damit beginnen, Ihre ausgehenden Nachrichten zu blockieren, oder dieselbe eigenständige Offline-E-Mail-Richtlinie kann für die Verarbeitung Ihrer ausgehenden Nachrichten verwendet werden (abhängig von der Definition der Richtlinie durch den Administrator).

Wenn Sie längere Zeit offline waren, können Sie manuell den Download von Richtlinien vom PGP Universal Server anfordern, wenn Sie wieder online sind. Wenn Sie wieder online sind, klicken Sie dazu in der Taskleiste auf das PGP Desktop-Symbol und wählen Sie die Option **Richtlinie aktualisieren** aus. Die aktuellsten Richtlinien werden vom PGP Universal Server heruntergeladen und alle Clientprotokolle werden auf den Server hochgeladen. Die Option zum manuellen Aktualisieren einer Richtlinie ist nur für verwaltete Benutzer verfügbar.

Wenn der PGP Universal Server-Administrator Ihnen die Verwendung von eigenständigen Richtlinien gestattet, finden Sie weitere Informationen unter *Neue Sicherheitsrichtlinien erstellen* (auf Seite 114).

Dienste und Richtlinien

Damit Sie Ihre ausgehenden Nachrichten mit PGP Desktop automatisch und transparent schützen können, müssen Sie zwei Begriffe kennen: Dienst und Richtlinie.

- **Dienst**: Informationen zu einem E-Mail-Konto auf dem System sowie zu den Richtlinien, die auf dieses Konto angewendet werden. In der Regel erstellt und konfiguriert PGP Desktop automatisch einen Dienst für jedes E-Mail-Konto auf dem System. In manchen Fällen sollten Sie einen Dienst manuell erstellen und konfigurieren.
- **Richtlinie**: Ein Satz von einer oder mehreren Anleitungen, die festlegen, welche Aktionen von PGP Desktop in bestimmten Situationen ausgeführt werden sollen. Richtlinien sind einem und oft auch mehreren Diensten zugeordnet (eine Richtlinie kann für verschiedene Dienste verwendet werden). Umgekehrt können einem Dienst mehrere Richtlinien zugewiesen werden, was auch oft der Fall ist.

Um festzulegen, wie eine bestimmte ausgehende E-Mail-Nachricht verarbeitet werden soll, überprüft PGP Desktop der Reihe nach (beginnend mit dem ersten Eintrag in der Liste) die Richtlinien, die für den jeweiligen Dienst konfiguriert wurden. Wenn eine entsprechende Richtlinie gefunden wird, werden die weiteren Richtlinien nicht überprüft. Stattdessen wird die gefundene Richtlinie angewendet.

Alle neuen Dienste werden mit den folgenden Standardrichtlinien erstellt:

- **Signier- und Verschlüsselungsschaltfläche**: Legt fest, dass E-Mail-Nachrichten sowohl signiert als auch verschlüsselt werden, wenn die Schaltflächen **Verschlüsseln** und **Signieren** in Microsoft Outlook 2002, 2003 oder 2007 aktiviert sind. Diese Richtlinie ist nur unter PGP Desktop für Windows verfügbar.
- **Signierschaltfläche**: Legt fest, dass E-Mail-Nachrichten signiert werden, wenn die Schaltfläche **Signieren** in Microsoft Outlook 2002, 2003 oder 2007 aktiviert ist. Diese Richtlinie ist nur unter PGP Desktop für Windows verfügbar.
- **Verschlüsselungsschaltfläche**: Legt fest, dass E-Mail-Nachrichten verschlüsselt werden, wenn die Schaltfläche **Verschlüsseln** in Microsoft Outlook 2002, 2003 oder 2007 aktiviert ist. Diese Richtlinie ist nur unter PGP Desktop für Windows verfügbar.
- **Adressenlisten-Administratoranforderungen**: Legt fest, dass Administratoranforderungen an Adressenlisten als Klartext gesendet werden, d. h. weder verschlüsselt noch signiert.
- **Adressenlisten-Sendevorgänge**: Legt fest, dass Sendevorgänge an Adressenlisten (für die Authentifizierung) signiert, jedoch nicht verschlüsselt gesendet werden.

- **Verschlüsselung erzwingen: [PGP] Vertraulich**: Legt fest, dass alle Nachrichten, die im E-Mail-Client als vertraulich gekennzeichnet sind oder den Text „[PGP]“ in der Betreffzeile enthalten, mit einem gültigen öffentlichen Schlüssel des Empfängers verschlüsselt werden **müssen**. Andernfalls können sie nicht gesendet werden.
- **Opportunistische Verschlüsselung**: Legt fest, dass alle Nachrichten, für die kein Verschlüsselungsschlüssel gefunden wird, unverschlüsselt (als Klartext) gesendet werden. Wenn diese Richtlinie als **letzte** Richtlinie in der Liste aufgeführt ist, wird sichergestellt, dass Nachrichten immer gesendet werden (wenn auch als Klartext), selbst wenn kein Schlüssel gefunden wird.

  Die Richtlinie „Opportunistische Verschlüsselung“ darf sich nur an letzter Stelle der Richtlinienliste befinden, da ihre Bedingungen immer zutreffen und PGP Desktop die Suche nach Richtlinien abbricht und die gefundene Richtlinie implementiert, sobald eine Übereinstimmung gefunden wird. Daher werden Richtlinien, die sich in der Liste unterhalb von „Opportunistische Verschlüsselung“ befinden, nie implementiert.

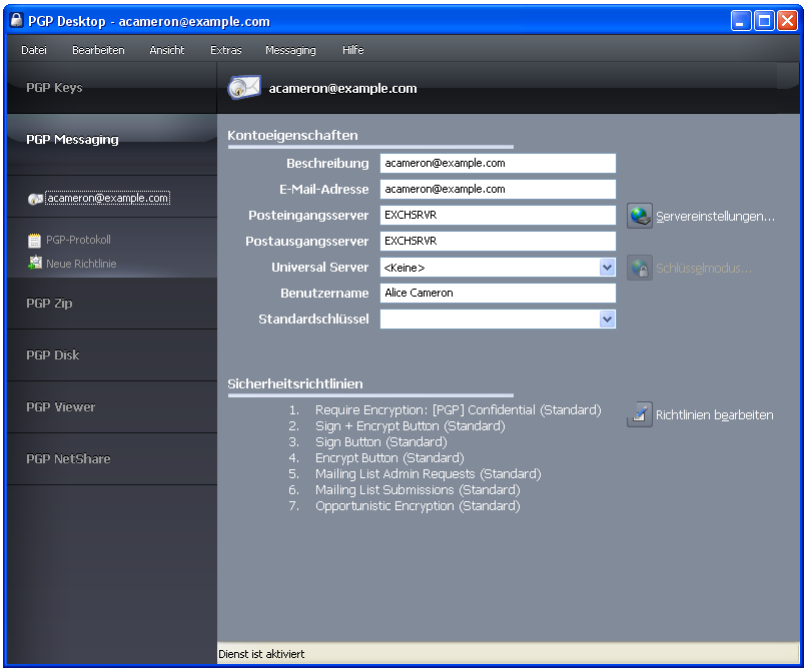
Hinweis: Die Standardrichtlinien können geändert, jedoch nicht gelöscht werden. Sie können allerdings deaktiviert und dann in der Richtlinienliste nach oben oder unten verschoben werden.

Dienste und Richtlinien anzeigen

▸ **So zeigen Sie Dienste und Richtlinien an**

1. Öffnen Sie PGP Desktop.
2. Klicken Sie auf das Bedienfeld „PGP Messaging“. Das Bedienfeld „PGP Messaging“ wird hervorgehoben. Alle aktuell konfigurierten Dienste werden oben im Bedienfeld „PGP-Messaging“ aufgeführt.

3 Klicken Sie auf einen Dienst, um die zugehörigen Kontoeigenschaften und Sicherheitsrichtlinien anzuzeigen. In diesem Abschnitt finden Sie Informationen darüber, welche Sicherheitsrichtlinie durchgesetzt wird. Wenn Sie in einer von einem PGP Universal Server verwalteten Umgebung arbeiten, werden die Sicherheitsrichtlinien vom Administrator festgelegt.



Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwaltete Umgebung einsetzen, werden abhängig von der Konfiguration der Richtlinie verschiedene Nachrichten und/oder Optionen über der Liste der Richtlinien angezeigt.

PGP Universal Server-Richtlinie:	**In PGP Desktop über der Liste der Richtlinien angezeigte Nachricht:**
Offline-Richtlinie ist auf Blockieren eingestellt	„Wenn der Server nicht erreicht werden kann, werden Nachrichten blockiert.“
Offline-Richtlinie ist auf Senden in Klartext eingestellt	„Wenn der Server nicht erreicht werden kann, werden Nachrichten im Klartext gesendet.“
Offline-Richtlinie ist auf eigenständigen Modus eingestellt	„Wenn der Server nicht erreicht werden kann, werden die eigenständigen Richtlinien durchgesetzt.“ Das Kontrollkästchen **Eigenständige Richtlinien anzeigen** wird angezeigt.
Richtlinie ist auf eigenständigen Modus eingestellt	„Die folgenden eigenständigen Richtlinien werden durchgesetzt.“

Falls der Administrator festgelegt hat, dass Sie Richtlinien ignorieren können, wird in allen Fällen das Kontrollkästchen **Serverrichtlinien mit lokalen Richtlinien überschreiben** angezeigt.

Neue Messaging-Dienste erstellen

Ein Dienst enthält Informationen zu einem E-Mail-Konto sowie zu den Sicherheitsrichtlinien, die auf ausgehende Nachrichten dieses E-Mail-Kontos angewendet werden sollen.

Wichtig: Gewöhnlich werden Dienste automatisch von PGP Desktop erstellt, wenn Sie Ihre E-Mail-Konten zum Senden oder Empfangen von Nachrichten verwenden. Wenn Sie selbst einen Dienst erstellen müssen, machen Sie sich zunächst mit den vorliegenden Anleitungen vertraut. Die fehlerhafte Konfiguration eines Dienstes führt u. U. zu Problemen beim Senden oder Empfangen von E-Mail-Nachrichten.

So erstellen Sie einen neuen Dienst

1. Öffnen Sie PGP Desktop und klicken Sie auf das Bedienfeld „PGP Messaging“. Das Bedienfeld „PGP Messaging“ wird hervorgehoben.
2. Klicken Sie im Bedienfeld „PGP Messaging“ auf **Neuer Messaging-Dienst**. Sie können auch **Messaging > Neuen Dienst erstellen auswählen.**

   Im Arbeitsbereich von PGP Messaging wird oben im Bildschirm der Text „Neuer Dienst“ angezeigt. Zudem werden die Kontoeigenschaften ohne Werte angezeigt und die Standardsicherheitsrichtlinien werden im Bereich „Sicherheitsrichtlinien“ aufgeführt.
3. Geben Sie im Bereich „Kontoeigenschaften“ im Feld **Beschreibung** einen Namen für den Dienst ein.
4. Geben Sie die E-Mail-Adresse in das Feld **E-Mail-Adresse** ein.
5. Geben Sie den Namen des Posteingangs- und des Postausgangsservers ein oder klicken Sie auf **Servereinstellungen**, wenn Sie erweiterte Optionen festlegen möchten. In diesem Fall wird das Dialogfeld „Servereinstellungen“ geöffnet.
6. Wählen Sie unter **Servertyp** den Servertyp für den neuen Dienst aus:
   - **Internet-E-Mail**: Für Benutzer, die PGP Desktop als eigenständige Lösung mit einer POP- oder IMAP-Verbindung nutzen.
   - **PGP Universal**: Für Benutzer von PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung. Wenden Sie sich an den PGP Universal Server-Administrator, wenn Sie weitere Informationen zu diesen Einstellungen benötigen.
   - **MAPI/Exchange**: Für Benutzer von PGP Desktop mit Microsoft Outlook als Client auf einem Microsoft Exchange/MAPI-Server. Wenden Sie sich an den E-Mail-Administrator, wenn Sie weitere Informationen zu diesen Einstellungen benötigen.

- **Lotus Notes**: Für Benutzer von PGP Desktop mit Lotus Notes als E-Mail-Client auf einem Lotus Domino-Server. Wenden Sie sich an den E-Mail-Administrator, wenn Sie weitere Informationen zu diesen Einstellungen benötigen.

Die verfügbaren Felder im Dialogfeld „Servereinstellungen“ variieren abhängig vom ausgewählten Servertyp.

Hinweis: Informationen zum manuellen Herstellen einer Verbindung mit einem PGP Universal Server finden Sie unter *Manuelle Bindung an einen PGP Universal Server* (auf Seite 359).

7 Geben Sie für **Mailserver für eingehende Nachrichten** folgende Daten ein:

- **Name**: Geben Sie den Namen des E-Mail-Servers ein, der eingehende Nachrichten verarbeitet.
- **Protokoll**: Wählen Sie das Protokoll aus, das zum Abrufen von Nachrichten auf dem Mailserver für eingehende Nachrichten verwendet wird.

  Bei Auswahl der Einstellung **Automatisch** (verfügbar für die Servertypen **Internet-E-Mail** und **PGP Universal Server**) wird automatisch erkannt, ob es sich um eine POP- oder IMAP-Verbindung handelt.

- **Port**: Behalten Sie die Standardeinstellung „Automatisch“ bei oder geben Sie einen Port an, über den die Verbindung zum Mailserver für eingehende Nachrichten hergestellt werden soll, um Nachrichten herunterzuladen (wenn Sie die Einstellungen **Internet-E-Mail** oder **PGP Universal Server** und dann entweder **POP** oder **IMAP** und nicht **Automatisch** ausgewählt haben).
- **SSL/TLS**: Geben Sie an, wie PGP Desktop mit dem E-Mail-Server kommunizieren soll. Folgende Optionen stehen zur Verfügung:
  - **Automatisch: Die PGP-Anwendung führt verschiedene Aktionen aus, um die Verbindung durch SSL/TLS zu schützen. Zunächst wird versucht, zum alternativen Port zu wechseln. Danach erfolgt ein Aufruf des Befehls „STARTTLS“ (sofern dieser vom Server unterstützt wird). Wenn keine dieser Vorgehensweisen erfolgreich ist, wird eine ungeschützte Verbindung zum Server hergestellt.**
  - **STARTTLS erforderlich: PGP Desktop erfordert, dass der Server den Befehl „STARTTLS“ unterstützt.**
  - **SSL erforderlich: PGP Desktop erfordert, dass der Server durch SSL geschützte Verbindungen zum angegebenen alternativen Port unterstützt.**
  - **Nicht versuchen: PGP Desktop versucht nicht, die Verbindung zum E-Mail-Server durch SSL/TLS zu schützen.**

- **Bei SSL/TLS-Verbindungsversuch durch E-Mail-Client warnen: Wenn diese Option ausgewählt ist, zeigt PGP Desktop eine Warnung an, wenn der E-Mail-Client versucht, eine SSL/TLS-Verbindung aufzubauen, da dies den E-Mail-Proxyvorgang durch PGP Desktop verhindern würde. (Diese Option ist standardmäßig aktiviert.)**

Achtung: Diese Option sollte nur aktiviert werden, wenn Sie sicher sind, dass der E-Mail-Server das SSL-Protokoll unterstützt. Auf diese Weise wird sichergestellt, dass PGP Desktop keine Nachrichten über ungeschützte Verbindungen sendet oder empfängt, falls beispielsweise ein Problem bei der Aushandlung des SSL-Protokolls für die Verbindung auftritt. **Wenn Sie diese Option aktivieren und der E-Mail-Server SSL nicht unterstützt, sendet oder empfängt PGP Desktop keine Nachrichten.**

Postausgangsserver (SMTP)

- **Name**: Geben Sie den Namen des E-Mail-Servers ein, der ausgehende Nachrichten verarbeitet.
- **Port**: Übernehmen Sie die Einstellung **Automatisch (465, 25)** oder geben Sie einen anderen Port auf dem Postausgangsserver an, über den Nachrichten gesendet werden.

  Diese Option steht nur dann für den Postausgangsserver zur Verfügung, wenn die Einstellungen für den Mailserver für eingehende Nachrichten die Auswahl dieser Option zulassen.
- **SSL/TLS**: Geben Sie an, wie PGP Desktop mit dem E-Mail-Server kommunizieren soll. Folgende Optionen stehen zur Verfügung:
  - **Automatisch: PGP Desktop führt verschiedene Aktionen aus, um die Verbindung durch SSL/TLS zu schützen. Zunächst wird versucht, zum alternativen Port zu wechseln. Danach erfolgt ein Aufruf des Befehls „STARTTLS“ (sofern dieser vom Server unterstützt wird). Wenn keine dieser Vorgehensweisen erfolgreich ist, wird eine ungeschützte Verbindung zum Server hergestellt.**
  - **STARTTLS erforderlich: PGP Desktop erfordert, dass der Server den Befehl „STARTTLS“ unterstützt.**
  - **SSL erforderlich: PGP Desktop erfordert, dass der Server durch SSL geschützte Verbindungen zum angegebenen alternativen Port unterstützt.**
  - **Nicht versuchen: PGP Desktop versucht nicht, die Verbindung zum E-Mail-Server durch SSL/TLS zu schützen.**
- **Bei SSL/TLS-Verbindungsversuch durch E-Mail-Client warnen: Wenn diese Option ausgewählt ist, zeigt PGP Desktop eine Warnung an, wenn der E-Mail-Client versucht, eine SSL/TLS-Verbindung aufzubauen, da dies den E-Mail-Proxyvorgang durch PGP Desktop verhindern würde. (Diese Option ist standardmäßig aktiviert.)**

Achtung: Diese Option sollte nur aktiviert werden, wenn Sie sicher sind, dass der E-Mail-Server das SSL-Protokoll unterstützt. Auf diese Weise wird sichergestellt, dass PGP Desktop keine Nachrichten über ungeschützte Verbindungen sendet oder empfängt, falls beispielsweise ein Problem bei der Aushandlung des SSL-Protokolls für die Verbindung auftritt. **Wenn Sie diese Option aktivieren und der E-Mail-Server SSL nicht unterstützt, sendet oder empfängt PGP Desktop keine Nachrichten.**

8 Klicken Sie abschließend auf **OK**.

9 Wählen Sie im Feld **Universal Server** **den Namen des PGP Universal Servers aus, der zum Schutz Ihrer E-Mail-Domäne verwendet wird.** **<Keine>** wird angezeigt, wenn Sie sich in einer E-Mail-Domäne befinden, die nicht durch einen PGP Universal Server geschützt wird. Wenn Ihre Domäne durch einen PGP Universal Server geschützt wird, dieser jedoch nicht in der Liste aufgeführt ist, wählen Sie **<Neu erstellen>** aus und geben Sie den Namen des PGP Universal Servers ein. Weitere Informationen erhalten Sie vom PGP Universal Server-Administrator.

10 Klicken Sie auf **Schlüsselmodus**. Das Dialogfeld für den Schlüsselverwaltungsmodus mit dem aktuellen Schlüsselmodus wird angezeigt. Klicken Sie bei Bedarf auf **Schlüssel zurücksetzen**, um den Einrichtungsassistenten für Schlüssel aufzurufen.

11 Klicken Sie auf **OK**.

12 Geben Sie im Feld **Benutzername** den Benutzernamen des E-Mail-Kontos ein.

13 Im Feld **Standardschlüssel** wird der aktuelle Schlüssel angezeigt.

- Wenn Sie PGP Desktop als eigenständiges Produkt verwenden, können Sie entweder den Standardschlüssel übernehmen oder (sofern verfügbar) einen anderen Schlüssel aus dem Menü auswählen.
- Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, kann der angezeigte Standardschlüssel nicht geändert werden. Falls Sie den Schlüssel ändern müssen, klicken Sie auf „Schlüsselmodus“ und führen Sie die Schritte zum Zurücksetzen des Schlüssels auf dem PGP Universal Server aus.

14 Aktivieren Sie das Kontrollkästchen **Passphrase dieses Schlüssels beim Anmelden zwischenspeichern**, wenn die Passphrase des Schlüsselpaars, das Sie gerade ausgewählt haben, bei der Anmeldung zwischengespeichert werden soll.

Wenn die Passphrase des Schlüssels nicht zwischengespeichert wird, müssen Sie sie jedes Mal eingeben, wenn Sie signierte Nachrichten versenden oder verschlüsselte Nachrichten empfangen.

15 Im Bereich **Durch [Servername] bereitgestellte Sicherheitsrichtlinien** werden die derzeit für Sie zutreffenden Sicherheitsrichtlinien angezeigt. Sie können die Standardsicherheitsrichtlinien übernehmen oder deaktivieren oder neue Richtlinien hinzufügen, wenn Sie PGP Desktop als eigenständiges Produkt verwenden. Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, werden wahrscheinlich abhängig von den vom PGP Universal Server-Administrator festgelegten Einstellungen andere Optionen angezeigt.

16 Wenn Sie eine Richtlinie bearbeitet haben, müssen Sie anschließend auf **Fertig** klicken. Ansonsten kann das Konto sofort verwendet werden. Sie müssen die Informationen nicht durch Klicken auf eine Schaltfläche speichern. Die Einstellungen wurden unmittelbar nach der Eingabe automatisch gespeichert.

Eigenschaften des Messaging-Dienstes bearbeiten

Achtung: Bevor Sie Änderungen an einem bestehenden Messaging-Dienst vornehmen, müssen Sie den E-Mail-Client beenden.

So ändern Sie die Kontoeigenschaften eines bestehenden Dienstes

1 Öffnen Sie PGP Desktop und klicken Sie auf das Bedienfeld „PGP Messaging“. Das Bedienfeld „PGP Messaging“ wird hervorgehoben.

2 Klicken Sie auf den Namen des Dienstes, dessen Kontoeigenschaften Sie bearbeiten möchten. Die Einstellungen für den ausgewählten Dienst werden im Arbeitsbereich von PGP Messaging angezeigt.

3 Nehmen Sie die gewünschten Änderungen an den Kontoeigenschaften des Dienstes vor. Weitere Informationen finden Sie unter *Neue Messaging-Dienste erstellen* (auf Seite 106).

Dienste deaktivieren oder aktivieren

Wenn Sie einen Dienst nur anhalten, jedoch nicht löschen möchten, da Sie ihn möglicherweise wieder benötigen, können Sie ihn deaktivieren. Dies bietet sich an, wenn PGP Desktop nur Nachrichten von bestimmten Konten verarbeiten soll. Wenn Sie sicher sind, dass Sie den Dienst nicht mehr benötigen, können Sie den Dienst löschen.

So deaktivieren oder aktivieren Sie einen bestehenden Dienst

1 Klicken Sie im Bedienfeld „PGP Messaging“ auf den Namen des Dienstes, den Sie deaktivieren möchten. Die Einstellungen für den Dienst werden im Arbeitsbereich „PGP Messaging“ angezeigt.

2 Führen Sie einen der folgenden Schritte aus:

- Deaktivieren Sie den Dienst, indem Sie **Messaging > Dienst deaktivieren** auswählen. Der Dienst wird deaktiviert.
- Aktivieren Sie den Dienst, indem Sie **Messaging > Dienst aktivieren** auswählen. Der Dienst wird aktiviert.

PGP Desktop informiert Sie darüber, dass die Änderung möglicherweise erst nach dem Neustart des E-Mail-Clients wirksam wird.

Tipp: Sie können Dienste deaktivieren, aktivieren und löschen, indem Sie im Bedienfeld „PGP Messaging“ mit der rechten Maustaste auf den Namen klicken und den gewünschten Befehl auswählen.

Dienste löschen

Wenn Sie sicher sind, dass Sie einen Messaging-Dienst nicht mehr benötigen, können Sie diesen Dienst aus PGP Desktop löschen.

▸ **So löschen Sie einen Dienst**

1 Klicken Sie auf den Namen des Dienstes, den Sie löschen möchten. Die Einstellungen für den Dienst werden im Arbeitsbereich „PGP Messaging“ angezeigt.

2 Wählen Sie **Messaging > Dienst löschen** aus. Der Dienst wird gelöscht.

Tipp: Sie können einen Dienst löschen, indem Sie im Bedienfeld „PGP Messaging“ mit der rechten Maustaste auf den Namen klicken und den gewünschten Befehl auswählen.

Mehrere Dienste

Einige E-Mail-Dienste und Internet-Dienstanbieter verwenden für einen einzelnen DNS-Namen mehrere E-Mail-Server, die der Reihe nach abgefragt werden. PGP Desktop kann in diesem Fall mehrere Messaging-Dienste für ein einzelnes E-Mail-Konto erstellen, da jeder E-Mail-Server getrennt betrachtet wird und somit seinen eigenen Messaging-Dienst erfordert.

PGP Desktop wird mit Platzhalterunterstützung für gängige E-Mail-Dienste ausgeliefert (z. B. *.yahoo.com und *.me.com bzw. *.mac.com). Falls Sie jedoch einen weniger gebräuchlichen E-Mail-Dienst verwenden oder sich die E-Mail-Server-Konfigurationen der Dienste ändern, könnte dieses Problem auftreten.

Wenn PGP Desktop mehrere Dienste für ein einzelnes E-Mail-Konto erstellt und Sie beim Überprüfen der Einstellungen feststellen, dass sich lediglich die E-Mail-Server unterscheiden (**mail1.beispiel.com für den ersten Dienst,** `mail2.beispiel.com` für den zweiten Dienst und `mail3.beispiel.com` für den dritten Dienst usw.), müssen Sie einen der Dienste möglicherweise manuell bearbeiten.

Die beste Lösung besteht darin, einen der Dienste manuell zu bearbeiten, sodass der E-Mail-Server-Eintrag für diesen Server mehrere E-Mail-Server unterstützen kann, die der Reihe nach abgefragt werden. Im oben aufgeführten Beispiel könnten Sie im Dialogfeld „Servereinstellungen“ den Servernamen für einen der Dienste in `mail*.beispiel.com` ändern und die anderen Dienste dann löschen.

Manche Konfigurationen können komplizierter sein und eine hiervon geringfügig abweichende Lösung erfordern. Wenn PGP Desktop beispielsweise Dienste mit den E-Mail-Servern pop.frodo.beispiel.com, smtp.bilbo.beispiel.com und mail.beispiel.com erstellen sollte, wäre die beste Platzhalterlösung ***.beispiel.com.**

Problembehebung bei PGP Messaging-Diensten

Standardmäßig ermittelt PGP Desktop automatisch die Einstellungen Ihres E-Mail-Kontos und erstellt einen PGP Messaging-Dienst, der als Proxy für den Messaging-Verkehr dieses Kontos dient.

Aufgrund der Vielzahl der möglichen E-Mail-Kontoeinstellungen und E-Mail-Server-Konfigurationen kann es jedoch vorkommen, dass ein von PGP Desktop automatisch eingerichteter Messaging-Dienst nicht ordnungsgemäß funktioniert.

Falls PGP Desktop einen Messaging-Dienst erstellt hat, der nicht Ihren Wünschen entspricht, können Sie das Problem möglicherweise anhand der folgenden Lösungsvorschläge beheben:

- Überprüfen Sie, ob eine Internetverbindung besteht und ob Sie E-Mail-Nachrichten senden und empfangen können, wenn PGP-Dienste angehalten wurden. Führen Sie dazu folgende Schritte aus:
  - Windows: Klicken Sie mit der rechten Maustaste auf das PGP Desktop-Symbol im Infobereich der Taskleiste und wählen Sie die Option **PGP-Dienste beenden** aus.
  - Mac OS X: Halten Sie die Wahltaste gedrückt und klicken Sie in der Menüleiste auf das PGP Desktop-Symbol. Wählen Sie die Option **Beenden** aus.

  Hinweis: Sie sollten den E-Mail-Client stets neu starten, wenn Sie die PGP-Dienste angehalten oder gestartet haben.
- Lesen Sie die Versionshinweise für die von Ihnen verwendete Version von PGP Desktop, um zu prüfen, ob es sich um ein bekanntes Problem handelt.

- Stellen Sie sicher, dass die SMTP-Authentifizierung für das E-Mail-Konto (in Ihrem E-Mail-Client) aktiviert ist. Dies wird empfohlen, damit PGP Desktop den Messaging-Verkehr über einen Proxy abwickeln kann. Wenn Sie nur über ein E-Mail-Konto verfügen und PGP Desktop nicht in einer von einem PGP Universal Server verwalteten Umgebung verwenden, ist keine SMTP-Authentifizierung erforderlich. Sie ist jedoch *erforderlich*, wenn Sie einen PGP Universal Server als SMTP-Server verwenden oder wenn Sie mehrere E-Mail-Konten auf dem gleichen SMTP-Server haben.
- Überprüfen Sie das PGP-Protokoll auf Einträge, die Hinweise auf die Art des Problems enthalten.
- Falls SSL/TLS im E-Mail-Client aktiviert ist und PGP Desktop den Messaging-Verkehr über einen Proxy abwickeln soll, müssen Sie die Option deaktivieren. (Der Schutz der Verbindung zwischen dem E-Mail-Client und dem E-Mail-Server wird dadurch *nicht* aufgehoben. PGP Desktop versucht standardmäßig automatisch, für jede ungeschützte Verbindung den SSL/TLS-Schutz zu aktivieren. Der E-Mail-Server muss SSL/TLS unterstützen, damit die Verbindung geschützt werden kann.)
- Wenn entweder **STARTTLS erfordern** oder **SSL erfordern** (in den SSL-/TLS-Einstellungen des Dialogfelds „Servereinstellungen“) ausgewählt ist, *muss* der E-Mail-Server SSL/TLS unterstützen. Andernfalls werden von PGP Desktop keine Nachrichten gesendet oder empfangen.
- Wenn das E-Mail-Konto keine Standard-Portnummern verwendet, stellen Sie sicher, dass diese Ports in den Einstellungen des Messaging-Dienstes enthalten sind.
- Falls PGP Desktop mehrere Messaging-Dienste für ein E-Mail-Konto erstellt, verwenden Sie einen Platzhalter für den Namen des E-Mail-Servers. Weitere Informationen finden Sie unter *Mehrere Dienste* (auf Seite 111).
- Löschen Sie den PGP Messaging-Dienst, der nicht ordnungsgemäß funktioniert, und senden und empfangen Sie E-Mail-Nachrichten. Der Messaging-Dienst wird von PGP Desktop neu erstellt.

Falls das Problem durch keine dieser Maßnahmen behoben werden kann, versuchen Sie Folgendes:

1. Löschen Sie den PGP Messaging-Dienst, der nicht ordnungsgemäß funktioniert.
2. Halten Sie alle PGP Desktop-Dienste an und beenden Sie PGP Desktop. So halten Sie die Dienste an
   - Windows: Klicken Sie mit der rechten Maustaste auf das PGP Desktop-Symbol im Infobereich der Taskleiste und wählen Sie die Option **PGP-Dienste beenden** aus.
   - Mac OS X: Halten Sie die Wahltaste gedrückt und klicken Sie in der Menüleiste auf das PGP Desktop-Symbol. Wählen Sie die Option **Beenden** aus.

3 Überprüfen Sie, ob eine Internetverbindung besteht und ob Sie E-Mail-Nachrichten senden und empfangen können, wenn PGP-Dienste angehalten wurden.

4 Öffnen Sie den E-Mail-Client und notieren Sie sich die Einstellungen des E-Mail-Kontos (einschließlich Benutzername, E-Mail-Adresse, Posteingangs- und Postausgangsserver, Protokoll des Posteingangsservers sowie alle E-Mail-Server-Ports, die nicht die Standardwerte verwenden).

5 Schließen Sie den E-Mail-Client und starten Sie PGP Desktop neu. Dadurch werden die PGP-Dienste neu gestartet:

- Windows: Starten Sie entweder den Computer neu oder öffnen Sie PGP Desktop über das Windows-Startmenü.
- Mac OS X: Starten Sie entweder den Computer neu oder öffnen Sie PGP Desktop.

6 Erstellen Sie anhand der zuvor notierten Kontoeinstellungen manuell einen PGP Messaging-Dienst.

7 Öffnen Sie den E-Mail-Client und senden und empfangen Sie E-Mail-Nachrichten.

8 Falls weiterhin Probleme mit einem PGP Messaging-Dienst auftreten, stehen folgende Informationsquellen zur Verfügung:

- *Website der PGP Corporation* (http://www.pgp.com)
- *PGP-Supportwebsite* (https://support.pgp.com)
- *PGP-Supportforen* (http://forum.pgp.com)

Neue Sicherheitsrichtlinien erstellen

Mit Sicherheitsrichtlinien wird gesteuert, wie ausgehende E-Mail-Nachrichten von PGP Desktop gehandhabt werden.

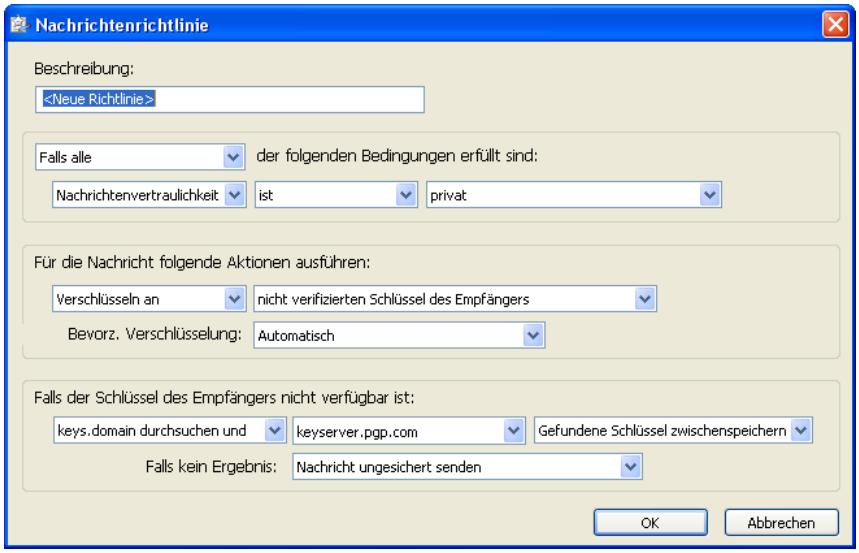
Hinweis: Wenn Sie eine neue Sicherheitsrichtlinie erstellen, wird eine Messaging-Sicherheitsrichtlinie und keine Adressenlisten-Richtlinie erstellt. Sie können keine neuen Adressenlisten-Richtlinien erstellen, Sie können jedoch die Standardrichtlinien für Adressenlisten bearbeiten.

So erstellen Sie eine neue Sicherheitsrichtlinie

1 Klicken Sie im Bedienfeld „PGP Messaging“ auf den Namen des Dienstes, für den Sie eine neue Sicherheitsrichtlinie erstellen möchten. Die Einstellungen für den Dienst werden zusammen mit der Liste der vorhandenen Sicherheitsrichtlinien im Arbeitsbereich von PGP Messaging angezeigt.

2 Führen Sie einen der folgenden Schritte aus:

- Klicken Sie im Bedienfeld von PGP Messaging auf **Neue Richtlinie**.
- Wählen Sie **Messaging > Neue Messaging-Richtlinie** aus. Das Dialogfeld „Nachrichtenrichtlinie“ wird angezeigt.



Wenn Ihre E-Mail-Domäne von einem PGP Universal Server geschützt ist, werden für die Richtlinieneinstellungen des Servers möglicherweise andere Felder als in der Abbildung angezeigt.

3 Geben Sie in das Feld **Beschreibung** einen aussagekräftigen Namen für die neue Richtlinie ein, die Sie erstellen.

4 Wählen Sie im ersten Abschnitt mit den Richtlinienbedingungen im Feld **Falls** eine der folgenden Optionen:

- **Falls beliebige**: Die Richtlinie wird angewendet, wenn eine der Bedingungen erfüllt ist.
- **Falls alle**: Die Richtlinie wird nur angewendet, wenn alle Bedingungen erfüllt sind.
- **Falls keine**: Die Richtlinie wird nur angewendet, wenn keine der Bedingungen erfüllt ist.

5 Wählen Sie im ersten Bedingungsfeld Folgendes aus:

- **Empfänger**: Die Richtlinie wird nur auf Nachrichten an den angegebenen Empfänger angewendet.
- **Empfängerdomäne**: Die Richtlinie wird nur auf E-Mail-Nachrichten in der angegebenen Empfängerdomäne angewendet.
- **Absender: Die Richtlinie wird nur auf Nachrichten mit der angegebenen Absenderadresse angewendet.**
- **Nachricht: Die Richtlinie wird nur auf Nachrichten mit dem angegebenen Signierungs- und/oder Verschlüsselungsstatus angewendet.**

- **Nachrichtenbetreff**: Die Richtlinie wird nur auf Nachrichten mit dem angegebenen Nachrichtenbetreff angewendet.
- **Nachrichtenkopf**: Die Richtlinie wird nur auf Nachrichten angewendet, bei denen die angegebene Kopfzeile die festgelegten Kriterien erfüllt. Beachten Sie, dass die im nächsten Abschnitt beschriebenen Bedingungen (ist, ist nicht, enthält usw.) für den Text gelten, der in das Textfeld eingegeben wird, das nach Auswahl von **Nachrichtenkopf** angezeigt wird.

Hinweis: Bei der Suche nach Nachrichtenköpfen in MAPI-E-Mail-Systemen können Sie nur nach den Kopfzeilen für Betreff, Vertraulichkeit, Priorität und Wichtigkeit suchen.

- **Nachrichtentext**: Die Richtlinie wird nur auf Nachrichten mit dem angegebenen Nachrichtentext angewendet.
- **Nachrichtengröße: Die Richtlinie wird nur auf Nachrichten mit der angegebenen Größe (in Byte) angewendet.**
- **Nachrichtenpriorität**: Die Richtlinie wird nur auf Nachrichten mit der angegebenen Nachrichtenpriorität angewendet.
- **Nachrichtenvertraulichkeit**: Die Richtlinie wird nur auf Nachrichten mit der angegebenen Nachrichtenvertraulichkeit angewendet.

6 Wählen Sie im zweiten Bedingungsfeld Folgendes aus:

- **ist**: Die Bedingung ist erfüllt, wenn der Text im ersten Bedingungsfeld mit dem Text im Textfeld *übereinstimmt*.
- **ist nicht**: Die Bedingung ist erfüllt, wenn der Text im ersten Bedingungsfeld mit dem Text im Textfeld *nicht übereinstimmt*.
- **enthält**: Die Bedingung ist erfüllt, wenn der Text im ersten Bedingungsfeld den Text im Textfeld *enthält*.
- **enthält nicht**: Die Bedingung ist erfüllt, wenn der Text im ersten Bedingungsfeld den Text im Textfeld *nicht enthält*.
- **beginnt mit**: Die Bedingung ist erfüllt, wenn der Text im ersten Bedingungsfeld mit dem Text im Textfeld *beginnt*.
- **endet mit**: Die Bedingung ist erfüllt, wenn der Text im ersten Bedingungsfeld mit dem Text im Textfeld *endet*.
- **stimmt mit Muster überein**: Die Bedingung ist erfüllt, wenn der Text im ersten Bedingungsfeld mit dem Textmuster im Textfeld *übereinstimmt*.
- **ist größer als**: Die Bedingung ist erfüllt, wenn die Nachrichtengröße *größer ist als* der im Textfeld eingegebene Text.
- **ist kleiner als:** Die Bedingung ist erfüllt, wenn die Nachrichtengröße *kleiner ist als* der im Textfeld eingegebene Text.

7 Wählen Sie im dritten Bedingungsfeld Folgendes aus:

- **Texteingabefeld**: Geben Sie den Text für die Übereinstimmungskriterien ein. Wenn Sie beispielsweise **Nachrichtengröße ist größer als** ausgewählt haben, geben Sie eine Zahl für die Größe der Nachricht ein.
- **normal**: Das Übereinstimmungskriterium für die Nachrichtenvertraulichkeit ist *normal*.
- **keine** bzw. **normal**: Das Übereinstimmungskriterium für die Nachrichtenvertraulichkeit ist *keine* (Mac OS X) bzw. *normal* (Windows).
- **persönlich**: Das Übereinstimmungskriterium für die Nachrichtenvertraulichkeit ist *persönlich*.
- **privat**: Das Übereinstimmungskriterium für die Nachrichtenvertraulichkeit ist *privat*.
- **vertraulich**: Das Übereinstimmungskriterium für die Nachrichtenvertraulichkeit ist *vertraulich*.
- **signiert**: Das Übereinstimmungskriterium für die Nachricht ist „signiert".
- **verschlüsselt**: Das Übereinstimmungskriterium für die Nachricht ist „verschlüsselt".
- **verschlüsselt an Schlüssel-ID**: Das Übereinstimmungskriterium für „verschlüsselt an Schlüssel-ID" (Sie müssen dann eine Schlüssel-ID in das angezeigte Textfeld eingeben).
- **niedrig**: Das Übereinstimmungskriterium für die Nachrichtenpriorität ist *niedrig*.
- **normal**: Das Übereinstimmungskriterium für die Nachrichtenpriorität ist *normal*.
- **hoch**: Das Übereinstimmungskriterium für die Nachrichtenpriorität ist *hoch*.

Erstellen Sie weitere Bedingungszeilen, indem Sie auf das Pluszeichen klicken.

8 Wählen Sie im Bereich **Für die Nachricht folgende Aktionen ausführen** im ersten Aktionsfeld Folgendes aus:

- **Klartext senden**: Gibt an, dass die Nachricht als Klartext gesendet werden soll, d. h. weder signiert noch verschlüsselt.
- **Signieren**: Gibt an, dass die Nachricht signiert werden soll.
- **Verschlüsseln an**: Gibt an, dass die Nachricht verschlüsselt werden soll.

9 Wählen Sie im zweiten Aktionsfeld Folgendes aus:

- **verifizierten Schlüssel des Empfängers**: Gewährleistet, dass die Nachricht nur an einen verifizierten Schlüssel des beabsichtigten Empfängers verschlüsselt werden kann.

- **nicht verifizierten Schlüssel des Empfängers**: Ermöglicht, dass die Nachricht an einen nicht verifizierten Schlüssel des beabsichtigten Empfängers verschlüsselt werden kann. Führt auch eine Verschlüsselung an einen möglicherweise vorhandenen verifizierten Schlüssel durch.
- **verifizierten End-to-End-Schlüssel des Empfängers**: Gewährleistet, dass die Nachricht nur an einen verifizierten End-to-End-Schlüssel des beabsichtigten Empfängers verschlüsselt werden kann. Ein End-to-End-Schlüssel befindet sich im alleinigen Besitz des jeweiligen Empfängers. In einer von einem PGP Universal Server verwalteten Umgebung ist dies ein CKM-Schlüssel (Client Key Mode). Im Gegensatz dazu befindet sich ein SKM-Schlüssel (Server Key Mode) im Besitz des PGP Universal Servers.

  Ob es sich um einen End-to-End-Schlüssel handelt, wird unter Windows im Dialogfeld „Schlüsseleigenschaften“ und unter Mac OS X im Dialogfeld „Schlüssel-Info“ im Feld **Gruppe** angezeigt. **Nein** bedeutet, dass es ein End-to-End-Schlüssel (d. h. nicht Teil einer Gruppe) *ist*, und **Ja** bedeutet, dass es sich *nicht* um einen End-to-End-Schlüssel handelt.
- **nicht verifizierten End-to-End-Schlüssel des Empfängers**: Ermöglicht, dass die Nachricht an einen nicht verifizierten End-to-End-Schlüssel des beabsichtigten Empfängers verschlüsselt werden kann. Führt auch eine Verschlüsselung an einen möglicherweise vorhandenen verifizierten Schlüssel durch.
- **eine Liste von Schlüsseln**: Gibt an, dass die Nachricht nur an Schlüssel in der Liste verschlüsselt werden kann.

Erstellen Sie weitere Aktionszeilen, indem Sie auf das Pluszeichen klicken.

10 Wählen Sie im Feld für die bevorzugte Nachrichtenverschlüsselung Folgendes aus:

- **Automatisch**: Das Nachrichtenverschlüsselungsformat wird von PGP Desktop ausgewählt. Dies ist die empfohlene Einstellung. Wählen Sie nur dann eine andere Option aus, wenn Sie genau wissen, warum Sie eines der anderen Nachrichtenverschlüsselungsformate benötigen.
- **PGP-partitioniert**: Legt „PGP-partitioniert“ als bevorzugtes Nachrichtenverschlüsselungsformat fest. Dieses Format gewährleistet die größte Rückwärtskompatibilität mit älteren PGP- und OpenPGP-Produkten.
- **PGP/MIME**: Legt „PGP/MIME“ als bevorzugtes Nachrichtenverschlüsselungsformat fest. Mit PGP/MIME kann die gesamte Nachricht, einschließlich Anlagen, in einem Durchgang verschlüsselt und signiert werden, was schneller ist und zu einer besseren Wiedergabe der gesamten Nachricht führt.
- **S/MIME**: Legt „S/MIME“ als bevorzugtes Nachrichtenverschlüsselungsformat fest. Wählen Sie „S/MIME“ aus, wenn Sie dieses Format verwenden müssen, obwohl der Benutzer über einen PGP-Schlüssel verfügt.

11 Wählen Sie im Bereich **Falls der Schlüssel des Empfängers nicht verfügbar ist** (bzw. unter Mac OS X im Bereich **Falls der Empfängerschlüssel nicht gefunden wird**) im ersten Feld **Folgendes aus:**

- **keys.domain durchsuchen und: Gibt an, dass die Suche sowohl in keys.domain als auch auf einem anderen, von Ihnen angegebenen Server durchgeführt wird.**
- **Suchen**: Ermöglicht die Suche nach einem entsprechenden Schlüssel, wenn am lokalen Schlüsselbund kein Schlüssel gefunden wird.
- **Nachricht als Klartext signieren: Gibt an, dass die Nachricht als Klartext gesendet werden soll, jedoch signiert wird.**
- **Nachricht ungesichert senden: Gibt an, dass die Nachricht als Klartext gesendet werden soll.**
- **Nachricht blockieren**: Gibt an, dass die Nachricht nicht gesendet werden soll, wenn kein entsprechender Schlüssel gefunden wird.

12 Wählen Sie im zweiten Feld Folgendes aus:

- **Alle Keyserver**: Gibt an, dass alle Keyserver, einschließlich des PGP Global Directory, nach einem entsprechenden Schlüssel durchsucht werden sollen.
- **PGP Global Directory bzw. keyserver.pgp.com**: Gibt an, dass nur das PGP Global Directory durchsucht wird.
- **[konfigurierte Keyserver]**: Gibt an, dass nur der Keyserver durchsucht wird, den Sie aus der Liste der aktuell konfigurierten Keyserver auswählen. Beachten Sie, dass andere Keyserver als das PGP Global Directory möglicherweise nicht verifizierte Schlüssel bereitstellen. Diese können nicht verwendet werden, wenn laut Richtlinie verifizierte Schlüssel erforderlich sind. Sofern Sie nicht genau wissen, warum ein bestimmter anderer Keyserver durchsucht werden soll, und Sie darauf vorbereitet sind, diese Schlüssel bei Bedarf manuell zum Verifizieren zu suchen, sollten Sie nur das PGP Global Directory durchsuchen. Diese Option ist nur unter Windows verfügbar.
- **Keyserver-Liste bearbeiten**: Ermöglicht Ihnen das Hinzufügen von Keyservern zur Liste der aktuell konfigurierten Keyserver. Diese Option ist nur unter Windows verfügbar.

13 Wählen Sie im letzten Feld Folgendes aus:

- **Gefundene Schlüssel zwischenspeichern**: Gibt an, dass ein gefundener Schlüssel zwischengespeichert werden soll. Die Schlüssel in diesem Zwischenspeicher werden automatisch zum Verifizieren signierter Nachrichten verwendet. Wenn Sie verifiziert wurden, werden Sie für die Verschlüsselung genutzt.
- **Zum Speichern gefundener Schlüssel auffordern**: Gibt an, dass PGP Desktop anfragen soll, ob Sie einen bestimmten gefundenen Schlüssel am lokalen Schlüsselbund speichern möchten.

- **Gefundene Schlüssel speichern**: Gibt an, dass gefundene Schlüssel automatisch am lokalen Schlüsselbund gespeichert werden sollen.

14 Wählen Sie in der Liste „Falls kein Ergebnis“ Folgendes aus:

- **Nachricht als Klartext signieren: Ermöglicht, dass Nachrichten, für die kein Verschlüsselungsschlüssel gefunden wird, signiert und als Klartext gesendet werden.**
- **Nachricht ungesichert senden: Die Nachricht wird nicht verschlüsselt.**
- **Nachricht blockieren: Verhindert, dass Nachrichten gesendet werden, für die kein Verschlüsselungsschlüssel gefunden wurde.**

15 Klicken Sie auf **OK**, wenn Sie alle Richtlinieneinstellungen konfiguriert haben. Die neue Richtlinie wird in der Liste der Sicherheitsrichtlinien angezeigt.

Reguläre Ausdrücke in Richtlinien

PGP Desktop unterstützt bei der Eingabe von Sicherheitsrichtlinien in Textfeldern die Verwendung von regulären Ausdrücken. Mit regulären Ausdrücken erzielen Sie über eine einzige Textzeichenfolge Übereinstimmungen mit mehreren Textzeichenfolgen.

Hinweis: Zusätzlich zu den folgenden Beispielen unterstützt PGP Desktop auch weitergehende reguläre Ausdrücke, die sich an Standardformaten orientieren. Das Kriterium „stimmt mit Muster überein“ bedeutet, dass der Suchbegriff mit einem regulären Ausdruck übereinstimmt.

Für einige Bedingungen von E-Mail-Richtlinien ist es erforderlich, dass ein Teil einer E-Mail-Nachricht mit einem Muster übereinstimmt. Die Muster in der Bedingung haben die Form eines regulären Ausdrucks. Ein regulärer Ausdruck ist eine Zeichenfolge, die das Format für einen Begriff darstellt, der übereinstimmen muss. Jeder Begriff, der dem Format des regulären Ausdrucks entspricht, ist eine Übereinstimmung.

Im Folgenden sind einige allgemeine Elemente von regulären Ausdrücken aufgeführt:

?	Gibt an, dass es eine oder keine Instanz des vorherigen Ausdrucks geben sollte.
+	Gibt an, dass es mindestens eine Instanz des vorherigen Ausdrucks gibt.
.	Entspricht einem beliebigen Einzelzeichen.
*	Gibt an, dass es keine, eine oder eine beliebige Anzahl von Instanzen des vorherigen Ausdrucks geben sollte.
[ ]	Entspricht einem beliebigen Einzelzeichen, das in der Klammer

	angegeben ist.
`[a-z]`	Entspricht einem kleingeschriebenen Buchstaben von a bis z.
`[1-9]`	Entspricht einer Ziffer von 1 bis 9.
`{n}`	Eine Folge von genau n Übereinstimmungen des Ausdrucks.

Im Folgenden sind Beispiele für reguläre Ausdrücke aufgeführt, die mit gebräuchlichen Objekten übereinstimmen, die in einer vertraulichen E-Mail-Nachricht enthalten sein können.

Daten	Beispiel	Regulärer Ausdruck
Telefonnummer	(555)555-4567	\(?[2-9][0-9]{2}[\)-.][2-9][0-9]{2}[-.][0-9]{4}
E-Mail-Adresse	joe@beispiel.com	[a-zA-Z0-9._%-]+@[a-zA-Z0-9.-]+\.[a-zA-Z]{2,6}
Kreditkartennummer	1234 1234 1234 1234	[1-9][0-9]{3} ?[0-9]{4} ?[0-9]{4} ?[0-9]{4}
Sozialversicherungsnummer	123-45-6789	[0-9]{3}-[0-9]{2}-[0-9]{4}
Ort, Abkürzung des Bundeslands	München, BY	.*, [A-Z][A-Z][A-Z]
Aus 1 bis 3 Zeichen bestehende Abkürzung des Bundeslands	BY	[A-Z][A-Z][A-Z]
Postleitzahl	12345	[0-9]{5}(-[0-9]{4})?
Eurobeträge mit vorangestelltem €-Zeichen	$3.95	\$[0-9]+.[0-9][0-9]
Datum, numerisch	2003-08-06	[0-9]{4}-[0-9]{2}-[0-9]{2}
Datum, alphanumerisch	3. Januar 2003	(Januar|Februar|März|April|Mai|Juni|Juli|August|September|Oktober|November|Dezember)\.? (3[0-1]|[1-2][0-9]|0?[0-9]), [0-9]{4}
HTTP-URL	http://www.beispiel.com	https?://(([012][0-9]{0,2}\.){3}[012][0-9]{0,2}|([a-zA-Z0-9]+\.)+[a-zA-Z0-9]{2,6})(/.*)?

Daten	Beispiel	Regulärer Ausdruck
IP-Adresse	123.123.123.123	([012][0-9]{0,2}\.){3}[012][0-9]{0,2}
Leerzeile		^$

Informationen und Beispiele zu Sicherheitsrichtlinien

Wenn Sie einen Dienst erstellen, werden automatisch mehrere Sicherheitsrichtlinien erstellt:

- Verschlüsselung erzwingen: [PGP] Vertraulich
- Signier- und Verschlüsselungsschaltfläche*
- Signierschaltfläche*
- Verschlüsselungsschaltfläche*
- Adressenlisten-Administratoranforderungen
- Adressenlisten-Sendevorgänge
- Opportunistische Verschlüsselung:

* *Diese Richtlinien sind nur in PGP Desktop für Windows verfügbar.*

Die Reihenfolge der Standardrichtlinienregeln ist wichtig. Achten Sie darauf, dass die oben beschriebene Reihenfolge genau eingehalten wird.

In diesem Abschnitt wird die Funktionsweise der Standardsicherheitsrichtlinien beschrieben. Darüber hinaus werden zwei Beispielsituationen beschrieben, für die Sie eine Sicherheitsrichtlinie erstellen könnten, sowie deren Konfiguration.

Hinweis: Wenn Sie Änderungen an den Standardrichtlinien vornehmen und die Standardeinstellungen wiederherstellen möchten, klicken Sie im Dialogfeld „Nachrichtenrichtlinie“ auf **Standard wiederherstellen** (Windows) oder auf **Zurücksetzen** (Mac OS X).

Standardrichtlinie „Verschlüsselungsschaltfläche“

„Verschlüsselungsschaltfläche“ ist eine der Standardsicherheitsrichtlinien, die von PGP Desktop automatisch für einen Dienst erstellt werden. Es gibt folgende Einstellungen für diese Standardrichtlinie:

- Falls: Falls alle
- Bedingungen: Nachrichtenkopf „X-PGP-Encrypt-Button“ enthält „selected“
- Aktionen: Verschlüsseln an verifizierten Schlüssel des Empfängers
- Bevorz. Verschlüsselung: Automatisch

- Falls der Schlüssel des Empfängers nicht verfügbar ist: keys.domain durchsuchen und keyserver.pgp.com - Gefundene Schlüssel zwischenspeichern

Falls kein Ergebnis: Nachricht blockieren Diese Regel sollte in der Richtlinienliste an 4. Stelle aufgeführt sein. **Hinweis:** Falls Sie von PGP Desktop für Windows Version 9.x aktualisiert haben, ist diese Richtlinie nicht automatisch eingeschlossen. Sie müssen sie daher manuell mit den oben angegebenen Einstellungen erstellen. Informationen zum Erstellen von neuen Richtlinien finden Sie unter *Neue Sicherheitsrichtlinien erstellen* (auf Seite 114). Falls Sie die Verschlüsselungsschaltfläche mit Microsoft Outlook nicht verwenden möchten, müssen Sie diese Richtlinie nicht erstellen.

Standardrichtlinie „Adressenlisten-Administratoranforderungen“

„Adressenlisten-Administratoranforderungen“ ist eine der Standardsicherheitsrichtlinien, die von PGP Desktop automatisch für einen Dienst erstellt werden.

Es gibt folgende Einstellungen für diese Standardrichtlinie:

- Falls: beliebige
- Bedingungen: Empfänger / stimmt mit Muster überein / .*-subscribe@.*, .*-unsubscribe@.*, .*-report@.*, .*-request@.*, .*-bounce@.*
- Aktionen: Klartext senden

Diese Regel sollte in der Richtlinienliste an 5. Stelle aufgeführt sein.

Standardrichtlinie „Adressenlisten-Sendevorgänge“

„Adressenlisten-Sendevorgänge“ ist eine der Standardsicherheitsrichtlinien, die von PGP Desktop automatisch für einen Dienst erstellt werden.

Es gibt folgende Einstellungen für diese Standardrichtlinie:

- Falls: beliebige
- Bedingungen: Empfänger / stimmt mit Muster überein / .*-users@.*, .*-bugs@.*, .*-docs@.*, .*-help@.*, .*-news@.*, .*-digest@.*, .*-list@.*, .*-devel@.*, .*-announce@.*
- Aktionen: Signieren

Bevorzugte Verschlüsselung: PGP-partitioniert Diese Regel sollte in der Richtlinienliste an 6. Stelle aufgeführt sein.

Standardrichtlinie „Opportunistische Verschlüsselung“

„Opportunistische Verschlüsselung“ ist eine der Standardsicherheitsrichtlinien, die von PGP Desktop automatisch für einen Dienst erstellt werden. Es gibt folgende Einstellungen für diese Standardrichtlinie:

- Falls: beliebige
- Bedingungen: Empfängerdomäne / ist / *
- Aktionen: Signieren / Verschlüsseln an / verifizierten Schlüssel des Empfängers
- Bevorzugte Verschlüsselung: Automatisch
- Schlüssel nicht gefunden: keys.domain durchsuchen und / keyserver.pgp.com / Gefundene Schlüssel zwischenspeichern
- Falls kein Ergebnis: Nachricht ungesichert senden

Diese Regel sollte in der Liste der Standardrichtlinien an 7. (letzter) Stelle aufgeführt sein.

Durch die opportunistische Verschlüsselung werden Nachrichten, für die ein verifizierter Schlüssel gefunden wird, signiert und verschlüsselt gesendet. Nachrichten, für die kein verifizierter Schlüssel gefunden wird, werden unverschlüsselt (als Klartext) gesendet. Auf diese Weise wird sichergestellt, dass Ihre Nachrichten gesendet werden, auch wenn einige als Klartext gesendet werden.

Diese Richtlinie sollte als letzter Eintrag in der Liste der Sicherheitsrichtlinien aufgeführt sein, da die Bedingungen der Richtlinie auf alle gesendeten Nachrichten zutreffen. Falls diese Richtlinie über einer anderen Richtlinie in der Liste angeordnet wird, erreicht PGP Desktop diese andere Richtlinie nie, sodass die Richtlinie nutzlos ist.

Standardrichtlinie „Verschlüsselung erzwingen: [PGP] Vertraulich“

„Verschlüsselung erzwingen: [PGP] Vertraulich“ ist eine der Standardsicherheitsrichtlinien, die von PGP Desktop automatisch für einen Dienst erstellt werden. Es gibt folgende Einstellungen für diese Standardrichtlinie:

- Falls: beliebige
- Bedingungen: Nachrichtenbetreff / enthält / [PGP] Nachrichtenvertraulichkeit / ist / vertraulich
- Aktionen: Signieren / Verschlüsseln an / verifizierten Schlüssel des Empfängers
- Bevorzugte Verschlüsselung: Automatisch
- Schlüssel nicht gefunden: keys.domain durchsuchen und / Alle Keyserver / Gefundene Schlüssel zwischenspeichern

Falls kein Ergebnis: Nachricht blockieren Diese Regel sollte in der Richtlinienliste an erster Stelle aufgeführt sein. Verschlüsselung erzwingen: [PGP] Vertraulich“ bewirkt, dass Nachrichten, die in der Betreffzeile den Text „[PGP]“ enthalten oder im E-Mail-Client als vertraulich gekennzeichnet sind, an einen verifizierten Schlüssel verschlüsselt werden müssen, um gesendet zu werden. Falls kein verifizierter Schlüssel gefunden werden kann, wird die Nachricht *nicht* gesendet.

Standardrichtlinie „Signier- und Verschlüsselungsschaltfläche“

„Signier- und Verschlüsselungsschaltfläche“ ist eine der Standardsicherheitsrichtlinien, die von PGP Desktop automatisch für einen Dienst erstellt werden. Es gibt folgende Einstellungen für diese Standardrichtlinie:

- Falls: Falls alle
- Bedingungen: Nachrichtenkopf „X-PGP-Sign-Button“ enthält „selected“; Nachrichtenkopf „X-PGP-Encrypt-Button“ enthält „selected“
- Aktionen: Signieren; Verschlüsseln an verifizierten Schlüssel des Empfängers
- Bevorz. Verschlüsselung: Automatisch
- Falls der Schlüssel des Empfängers nicht verfügbar ist: keys.domain durchsuchen und keyserver.pgp.com - Gefundene Schlüssel zwischenspeichern

Falls kein Ergebnis: Nachricht blockieren Diese Regel sollte in der Richtlinienliste an 2. Stelle aufgeführt sein. **Hinweis:** Falls Sie von PGP Desktop für Windows Version 9.x aktualisiert haben, ist diese Richtlinie nicht automatisch eingeschlossen. Sie müssen sie daher manuell mit den oben angegebenen Einstellungen erstellen. Informationen zum Erstellen von neuen Richtlinien finden Sie unter *Neue Sicherheitsrichtlinien erstellen* (auf Seite 114). Falls Sie die Verschlüsselungsschaltfläche mit Microsoft Outlook nicht verwenden möchten, müssen Sie diese Richtlinie nicht erstellen.

Standardrichtlinie „Signierschaltfläche“

„Signierschaltfläche“ ist eine der Standardsicherheitsrichtlinien, die von PGP Desktop automatisch für einen Dienst erstellt werden. Es gibt folgende Einstellungen für diese Standardrichtlinie:

- Falls: Falls alle
- Bedingungen: Nachrichtenkopf „X-PGP-Sign-Button“ enthält „selected“
- Aktionen: Signieren

Bevorz. Verschlüsselung: Automatisch Diese Regel sollte in der Richtlinienliste an 3. Stelle aufgeführt sein. **Hinweis:** Falls Sie von PGP Desktop für Windows Version 9.x aktualisiert haben, ist diese Richtlinie nicht automatisch eingeschlossen. Sie müssen sie daher manuell mit den oben angegebenen Einstellungen erstellen. Informationen zum Erstellen von neuen Richtlinien finden Sie unter *Neue Sicherheitsrichtlinien erstellen* (auf Seite 114). Falls Sie die Verschlüsselungsschaltfläche mit Microsoft Outlook nicht verwenden möchten, müssen Sie diese Richtlinie nicht erstellen.

Beispiel für eine Richtlinie zur Erzwingung der Verschlüsselung an <Domäne>

Wenn Sie die Richtlinie „Opportunistische Verschlüsselung“ mit den Standardeinstellungen verwenden und die Richtlinie am Ende der Liste aufgeführt ist, werden Nachrichten, für die kein verifizierter Schlüssel gefunden wird, als Klartext übermittelt. Auf diese Weise wird sichergestellt, dass alle Nachrichten gesendet werden. Es bedeutet jedoch auch, dass einige Nachrichten möglicherweise unverschlüsselt gesendet werden.

Falls es bestimmte Domänen gibt, für die das Senden als Klartext nicht in Frage kommt, können Sie eine Sicherheitsrichtlinie erstellen, derzufolge eine Nachricht verschlüsselt und/oder signiert werden muss oder andernfalls *nicht* gesendet wird. Wenn Sie diese Richtlinie erstellen, achten Sie darauf, sie in der Liste über der Richtlinie „Opportunistische Verschlüsselung“ anzuordnen.

- Falls: beliebige
- Bedingungen: Empfängerdomäne / ist / beispiel.com
- Aktionen: Verschlüsseln an / verifizierten Schlüssel des Empfängers
- Bevorzugte Verschlüsselung: Automatisch
- Schlüssel nicht gefunden: keys.domain durchsuchen und / Alle Keyserver / Gefundene Schlüssel zwischenspeichern
- Falls kein Ergebnis: Nachricht blockieren

Diese Sicherheitsrichtlinie entspricht zum Teil der Richtlinie „Verschlüsselung erzwingen: [PGP] Vertraulich“, da sie vorsieht, dass eine Nachricht nur verschlüsselt gesendet werden kann. Das Auswahlkriterium ist jedoch nicht, ob die Nachricht als vertraulich gekennzeichnet ist, sondern ob die E-Mail-Domäne des Empfängers „beispiel.com“ lautet. Durch die Verwendung dieser Richtlinie wird sichergestellt, dass alle Nachrichten an „beispiel.com“ mit einem verifizierten Schlüssel verschlüsselt sind oder andernfalls nicht gesendet werden.

Beispiel für eine Richtlinie zum Signieren und Senden als Klartext an eine bestimmte Domäne

Falls Sie regelmäßig E-Mail-Nachrichten an eine Domäne senden, für die Sie alle Nachrichten zwar signieren, jedoch nicht verschlüsseln möchten, sollten Sie eine Richtlinie für die Domäne erstellen.

- Falls: beliebige
- Bedingungen: Empfängerdomäne / ist / beispiel.com
- Aktionen: Signieren
- Bevorzugte Verschlüsselung: Automatisch

Mit der Sicherheitsrichtlinienliste arbeiten

Es stehen verschiedene Möglichkeiten für die Sicherheitsrichtlinien in der Sicherheitsrichtlinienliste zur Verfügung. Beispielsweise können Sie eine Richtlinie bearbeiten, eine neue Richtlinie hinzufügen (siehe *Neue Sicherheitsrichtlinien erstellen* (auf Seite 114)) eine Richtlinie löschen oder die Reihenfolge der Richtlinien in der Liste ändern.

Sicherheitsrichtlinien bearbeiten

▸ **So bearbeiten Sie eine bestehende Sicherheitsrichtlinie**

1. Öffnen Sie PGP Desktop und klicken Sie auf das Bedienfeld „PGP Messaging“. Das Bedienfeld „PGP Messaging“ wird hervorgehoben.
2. Klicken Sie im Bedienfeld „PGP Messaging“ auf den Namen des Dienstes mit der Sicherheitsrichtlinie, die Sie bearbeiten möchten. Die Eigenschaften des ausgewählten Dienstes werden im Arbeitsbereich von PGP Messaging angezeigt.
3. Klicken Sie auf **Richtlinien bearbeiten**.
4. Wählen Sie die Sicherheitsrichtlinie aus, die Sie bearbeiten möchten, und führen Sie dann einen der folgenden Schritte aus:

- Bearbeiten Sie die Richtlinie, indem Sie auf **Richtlinie bearbeiten** klicken. Das Dialogfeld „Nachrichtenrichtlinie“ wird mit den aktuellen Einstellungen für die angegebene Richtlinie geöffnet. Nehmen Sie die gewünschten Änderungen an der Richtlinie vor. Informationen zu den Feldern im Dialogfeld „Nachrichtenrichtlinie“ finden Sie unter *Neue Sicherheitsrichtlinien erstellen* (auf Seite 114). Nachdem Sie die gewünschten Änderungen vorgenommen haben, klicken Sie auf **OK**, um das Dialogfeld „Nachrichtenrichtlinie“ zu schließen. Die angegebene Sicherheitsrichtlinie wird geändert.
- Löschen Sie die Richtlinie, indem Sie auf **Richtlinie entfernen** klicken.
- Erstellen Sie eine Kopie der Richtlinie (als Grundlage für eine neue Richtlinie), indem Sie auf **Richtlinie duplizieren** klicken.
- Verschieben Sie die Richtlinie in der Liste nach oben oder nach unten (d. h. ändern Sie die Reihenfolge, in der Richtlinien angewendet werden), indem Sie auf **Nach oben** oder **Nach unten** klicken.

Standardrichtlinien können angezeigt, geändert und deaktiviert, jedoch nicht gelöscht werden.

5 Klicken Sie auf **Fertig**.

Adressenlisten-Richtlinien bearbeiten

▸ **So bearbeiten Sie eine standardmäßige Adressenlisten-Richtlinie**

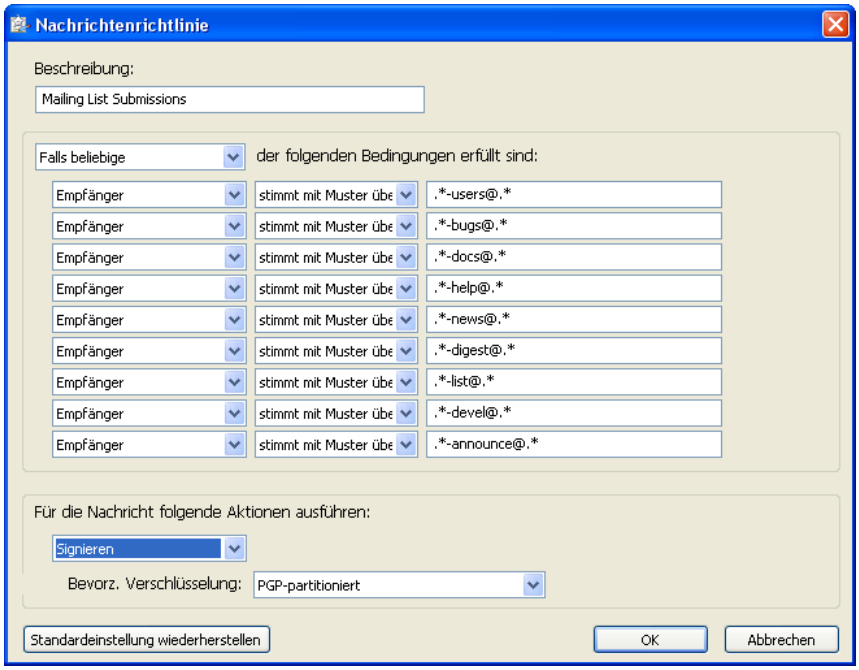
1 Öffnen Sie PGP Desktop und klicken Sie auf das Bedienfeld „PGP Messaging“. Das Bedienfeld „PGP Messaging“ wird hervorgehoben.

2 Klicken Sie im Bedienfeld „PGP Messaging“ auf den Namen des Dienstes mit der Sicherheitsrichtlinie, die Sie bearbeiten möchten. Die Eigenschaften des ausgewählten Dienstes werden im Arbeitsbereich von PGP Messaging angezeigt.

3 Klicken Sie auf die Schaltfläche **Richtlinien bearbeiten**.

4 Klicken Sie in der Liste der Sicherheitsrichtlinien auf die Adressenlisten-Richtlinie, die Sie bearbeiten möchten. Die ausgewählte Richtlinie wird hervorgehoben.

5 Klicken Sie auf **Richtlinie bearbeiten**. Das Dialogfeld „Nachrichtenrichtlinie“ wird mit den aktuellen Einstellungen für die angegebene Richtlinie geöffnet.



Die Standardrichtlinien können angezeigt, geändert und deaktiviert, jedoch nicht gelöscht werden.

6 Nehmen Sie die gewünschten Änderungen an der Richtlinie vor. Wählen Sie im ersten Feld Folgendes aus:

- **Falls beliebige**: Die Richtlinie wird angewendet, wenn eine der Bedingungen erfüllt ist.
- **Falls alle**: Die Richtlinie wird nur angewendet, wenn alle Bedingungen erfüllt sind.
- **Falls keine**: Die Richtlinie wird nur angewendet, wenn keine der Bedingungen erfüllt ist.

7 Wählen Sie im ersten Bedingungsfeld Folgendes aus:

- **Empfänger**: Die Richtlinie wird nur auf Nachrichten an den angegebenen Empfänger angewendet.
- **Empfängerdomäne**: Die Richtlinie wird nur auf E-Mail-Nachrichten in der angegebenen Empfängerdomäne angewendet.
- **Absender: Die Richtlinie wird nur auf Nachrichten mit der angegebenen Absenderadresse angewendet.**
- **Nachricht: Die Richtlinie wird nur auf Nachrichten mit dem angegebenen Signierungs- und/oder Verschlüsselungsstatus angewendet.**

- **Nachrichtenbetreff**: Die Richtlinie wird nur auf Nachrichten mit dem angegebenen Nachrichtenbetreff angewendet.
- **Nachrichtenkopf**: Die Richtlinie wird nur auf Nachrichten angewendet, bei denen die angegebene Kopfzeile die festgelegten Kriterien erfüllt. Beachten Sie, dass die im nächsten Abschnitt beschriebenen Bedingungen (ist, ist nicht, enthält usw.) für den Text gelten, der in das Textfeld eingegeben wird, das nach Auswahl von **Nachrichtenkopf** angezeigt wird.

Hinweis: Die Suche nach Nachrichtenköpfen in Lotus Notes- und MAPI-E-Mail-Systemen ist nicht implementiert, da Nachrichten in diesen Systemen keinen Nachrichtenkopf aufweisen.

- **Nachrichtentext**: Die Richtlinie wird nur auf Nachrichten mit dem angegebenen Nachrichtentext angewendet.
- **Nachrichtengröße: Die Richtlinie wird nur auf Nachrichten mit der angegebenen Größe (in Byte) angewendet.**
- **Nachrichtenpriorität**: Die Richtlinie wird nur auf Nachrichten mit der angegebenen Nachrichtenpriorität angewendet.
- **Nachrichtenvertraulichkeit**: Die Richtlinie wird nur auf Nachrichten mit der angegebenen Nachrichtenvertraulichkeit angewendet.

8 Wählen Sie im zweiten Bedingungsfeld Folgendes aus:

- **ist**: Die Bedingung ist erfüllt, wenn der Text im ersten Bedingungsfeld mit dem Text im Textfeld *übereinstimmt*.
- **ist nicht**: Die Bedingung ist erfüllt, wenn der Text im ersten Bedingungsfeld mit dem Text im Textfeld *nicht übereinstimmt*.
- **enthält**: Die Bedingung ist erfüllt, wenn der Text im ersten Bedingungsfeld den Text im Textfeld *enthält*.
- **enthält nicht**: Die Bedingung ist erfüllt, wenn der Text im ersten Bedingungsfeld den Text im Textfeld *nicht enthält*.
- **beginnt mit**: Die Bedingung ist erfüllt, wenn der Text im ersten Bedingungsfeld mit dem Text im Textfeld *beginnt*.
- **endet mit**: Die Bedingung ist erfüllt, wenn der Text im ersten Bedingungsfeld mit dem Text im Textfeld *endet*.
- **stimmt mit Muster überein**: Die Bedingung ist erfüllt, wenn der Text im ersten Bedingungsfeld mit dem Textmuster im Textfeld *übereinstimmt*.

9 Geben Sie im dritten Bedingungsfeld in das Textfeld den Text für die Übereinstimmungskriterien ein.

10 Wählen Sie im Bereich „Für die Nachricht folgende Aktionen ausführen“ im ersten Aktionsfeld Folgendes aus:

- **Klartext senden**: Gibt an, dass die Nachricht als Klartext gesendet werden soll, d. h. weder signiert noch verschlüsselt.

- **Signieren**: Gibt an, dass die Nachricht signiert werden soll.
- **Verschlüsseln an**: Gibt an, dass die Nachricht verschlüsselt werden soll.

11 Wählen Sie im zweiten Aktionsfeld Folgendes aus:

- **verifizierten Schlüssel des Empfängers**: Gewährleistet, dass die Nachricht nur an einen verifizierten Schlüssel des beabsichtigten Empfängers verschlüsselt werden kann.
- **nicht verifizierten Schlüssel des Empfängers**: Ermöglicht, dass die Nachricht an einen nicht verifizierten Schlüssel des beabsichtigten Empfängers verschlüsselt werden kann.

verifizierten End-to-End-Schlüssel des Empfängers: Gewährleistet, dass die Nachricht nur an einen verifizierten End-to-End-Schlüssel des beabsichtigten Empfängers verschlüsselt werden kann. Ein End-to-End-Schlüssel befindet sich im alleinigen Besitz des jeweiligen Empfängers. In einer von einem PGP Universal Server verwalteten Umgebung ist dies ein CKM-Schlüssel (Client Key Mode). Im Gegensatz dazu befindet sich ein SKM-Schlüssel (Server Key Mode) im Besitz des PGP Universal Servers.

Ob es sich um einen End-to-End-Schlüssel handelt, wird unter Windows im Dialogfeld „Schlüsseleigenschaften“ und unter Mac OS X im Dialogfeld „Schlüssel-Info“ im Feld **Gruppe** angezeigt. **Nein** bedeutet, dass es ein End-to-End-Schlüssel (d. h. nicht Teil einer Gruppe) *ist*, und **Ja** bedeutet, dass es sich *nicht* um einen End-to-End-Schlüssel handelt.

- **nicht verifizierten End-to-End-Schlüssel des Empfängers**: Ermöglicht, dass die Nachricht an einen nicht verifizierten End-to-End-Schlüssel des beabsichtigten Empfängers verschlüsselt werden kann.
- **eine Liste von Schlüsseln**: Gibt an, dass die Nachricht nur an Schlüssel in der Liste verschlüsselt werden kann.

12 Wählen Sie im Feld für die bevorzugte Nachrichtenverschlüsselung Folgendes aus:

- **Automatisch**: Das Nachrichtenverschlüsselungsformat wird von PGP Desktop ausgewählt. Dies ist die empfohlene Einstellung. Wählen Sie nur dann eine andere Option aus, wenn Sie genau wissen, warum Sie eines der anderen Nachrichtenverschlüsselungsformate benötigen.
- **PGP-partitioniert**: Legt „PGP-partitioniert“ als bevorzugtes Nachrichtenverschlüsselungsformat fest. Dieses Format gewährleistet die größte Rückwärtskompatibilität mit älteren PGP- und OpenPGP-Produkten.
- **PGP/MIME**: Legt „PGP/MIME“ als bevorzugtes Nachrichtenverschlüsselungsformat fest. Mit PGP/MIME kann die gesamte Nachricht, einschließlich Anlagen, in einem Durchgang verschlüsselt und signiert werden, was schneller ist und zu einer besseren Wiedergabe der gesamten Nachricht führt.

- **S/MIME**: Legt „S/MIME“ als bevorzugtes Nachrichtenverschlüsselungsformat fest. Wählen Sie „S/MIME“ aus, wenn Sie dieses Format verwenden müssen, obwohl der Benutzer über einen PGP-Schlüssel verfügt.

13 Wählen Sie im Bereich **Falls der Schlüssel des Empfängers nicht verfügbar ist** im ersten Feld **Folgendes aus:**

- **keys.domain durchsuchen und**: Gibt an, dass die Suche sowohl in keys.domain als auch auf einem anderen, von Ihnen angegebenen Server durchgeführt wird.
- **Suchen**: Ermöglicht die Suche nach einem entsprechenden Schlüssel, wenn am lokalen Schlüsselbund kein Schlüssel gefunden wird.
- **Nachricht als Klartext signieren**: Gibt an, dass die Nachricht als Klartext gesendet werden soll, jedoch signiert wird.
- **Nachricht ungesichert senden**: Gibt an, dass die Nachricht als Klartext gesendet werden soll.
- **Nachricht blockieren**: Gibt an, dass die Nachricht nicht gesendet werden soll, wenn kein entsprechender Schlüssel gefunden wird.

14 Wählen Sie im zweiten Feld Folgendes aus:

- **Alle Keyserver**: Gibt an, dass alle Keyserver, einschließlich des PGP Global Directory, nach einem entsprechenden Schlüssel durchsucht werden sollen.
- **PGP Global Directory bzw. keyserver.pgp.com**: Gibt an, dass nur das PGP Global Directory durchsucht wird.
- **[konfigurierte Keyserver]**: Gibt an, dass nur der Keyserver durchsucht wird, den Sie aus der Liste der aktuell konfigurierten Keyserver auswählen. Beachten Sie, dass andere Keyserver als das PGP Global Directory möglicherweise nicht verifizierte Schlüssel bereitstellen. Diese können nicht verwendet werden, wenn laut Richtlinie verifizierte Schlüssel erforderlich sind. Sofern Sie nicht genau wissen, warum ein bestimmter anderer Keyserver durchsucht werden soll, und Sie darauf vorbereitet sind, diese Schlüssel bei Bedarf manuell zum Verifizieren zu suchen, sollten Sie nur das PGP Global Directory durchsuchen. Diese Option ist nur unter Windows verfügbar.
- **Keyserver-Liste bearbeiten**: Ermöglicht Ihnen das Hinzufügen von Keyservern zur Liste der aktuell konfigurierten Keyserver. Diese Option ist nur unter Windows verfügbar.

15 Wählen Sie im letzten Feld Folgendes aus:

- **Gefundene Schlüssel zwischenspeichern**: Gibt an, dass ein gefundener Schlüssel zwischengespeichert werden soll. Die Schlüssel in diesem Zwischenspeicher werden automatisch zum Verifizieren signierter Nachrichten verwendet. Wenn Sie verifiziert wurden, werden Sie für die Verschlüsselung genutzt.

- **Zum Speichern gefundener Schlüssel auffordern**: Gibt an, dass PGP Desktop anfragen soll, ob Sie einen bestimmten gefundenen Schlüssel am lokalen Schlüsselbund speichern möchten.
- **Gefundene Schlüssel speichern**: Gibt an, dass gefundene Schlüssel automatisch am lokalen Schlüsselbund gespeichert werden sollen.

16 Wählen Sie in der Liste „Falls kein Ergebnis“ Folgendes aus:

- **Nachricht als Klartext signieren**: Ermöglicht, dass Nachrichten, für die kein Verschlüsselungsschlüssel gefunden wird, signiert und als Klartext gesendet werden.
- **Nachricht ungesichert senden**: Die Nachricht wird nicht verschlüsselt.
- **Nachricht blockieren**: Verhindert, dass Nachrichten gesendet werden, für die kein Verschlüsselungsschlüssel gefunden wurde.

17 Nachdem Sie die gewünschten Änderungen vorgenommen haben, klicken Sie auf **OK**, um das Dialogfeld „Nachrichtenrichtlinie“ zu schließen. Die angegebene Sicherheitsrichtlinie wird geändert.

Sicherheitsrichtlinien löschen

So löschen Sie eine bestehende Sicherheitsrichtlinie

1 Klicken Sie im Bedienfeld „PGP Messaging“ auf den Namen des Dienstes mit der Sicherheitsrichtlinie, die Sie löschen möchten. Die Eigenschaften des ausgewählten Dienstes werden im Arbeitsbereich von PGP Messaging angezeigt.

2 Klicken Sie auf **Richtlinien bearbeiten**.

3 Klicken Sie in der Liste der Sicherheitsrichtlinien auf die Richtlinie, die Sie löschen möchten. Die angegebene Richtlinie wird hervorgehoben.

4 Klicken Sie auf **Richtlinie entfernen**. Ein PGP Desktop-Bestätigungsdialogfeld wird angezeigt.

5 Klicken Sie auf **Richtlinie löschen**, um die Richtlinie zu löschen, oder auf **OK**, um sie zu deaktivieren. Die ausgewählte Sicherheitsrichtlinie wird gelöscht oder deaktiviert.

6 Klicken Sie auf **Fertig**.

Hinweis: Standardrichtlinien können deaktiviert, jedoch nicht gelöscht werden.

Reihenfolge der Richtlinien in der Liste ändern

▸ **So ändern Sie die Reihenfolge der Richtlinien in der Sicherheitsrichtlinienliste**

1. Klicken Sie im Bedienfeld „PGP Messaging“ auf den Namen des Dienstes mit der Sicherheitsrichtlinie, deren Reihenfolge Sie ändern möchten. Die Eigenschaften des ausgewählten Dienstes werden im Arbeitsbereich von PGP Messaging angezeigt.
2. Klicken Sie auf **Richtlinien bearbeiten**.
3. Klicken Sie in der Sicherheitsrichtlinienliste auf die Richtlinie, deren Reihenfolge Sie in der Liste ändern möchten. Die angegebene Richtlinie wird hervorgehoben.
4. Klicken Sie auf **Nach oben** oder **Nach unten**, bis sich die Richtlinie an der gewünschten Position in der Liste befindet. Achten Sie darauf, dass die Richtlinie **Opportunistische Verschlüsselung** an letzter Stelle in der Liste aufgeführt ist. Alle danach folgenden Richtlinien werden nicht implementiert.
5. Klicken Sie auf **Fertig**.

PGP Desktop und SSL

Wenn Sie PGP Desktop verwenden, zielt die PGP Corporation darauf ab, Ihre Daten nach Möglichkeit automatisch zu sichern. Dazu gehört der Schutz der Daten bei der Übertragung zwischen dem E-Mail-Client und dem E-Mail-Server.

Tipp: SSL ist die Abkürzung für Secure Sockets Layer, ein kryptografisches Protokoll zum Sichern der Kommunikation zwischen zwei Geräten. In diesem Fall sichert es die Kommunikation zwischen dem E-Mail-Client bzw. PGP Desktop und dem E-Mail-Server.

Abhängig von den jeweiligen Bedingungen schützt PGP Desktop die Daten auf dem Übertragungsweg zum und vom E-Mail-Server auf verschiedene Weise. Die folgenden Informationen gelten nur, wenn Sie im Dialogfeld „Servereinstellungen“ für die SSL/TLS-Einstellung die Option **Automatisch** (Standardeinstellung) ausgewählt haben:

- **Wenn die Verbindung nicht durch SSL geschützt ist:** Wenn die Verbindung zwischen dem E-Mail-Client und dem E-Mail-Server nicht durch SSL geschützt ist, versucht PGP Desktop automatisch, für diese Verbindung SSL zu verwenden (d. h. die Anwendung kommuniziert mit dem E-Mail-Server und verwendet SSL, wenn dies vom E-Mail-Server unterstützt wird).

Wenn der E-Mail-Server SSL nicht unterstützt, werden die Nachrichten, die von PGP Desktop während der Sitzung gesendet und empfangen werden, über eine ungeschützte Verbindung übertragen. PGP Desktop versucht grundsätzlich, eine SSL-Verbindung aufzubauen, unabhängig davon, ob PGP Desktop die Nachrichten verschlüsselt oder entschlüsselt. Nachrichten, die von PGP Desktop verschlüsselt wurden, können über eine durch SSL geschützte Verbindung oder über eine ungeschützte Verbindung gesendet und empfangen werden.

Hinweis: Bei einer ungeschützten Verbindung zum E-Mail-Server versucht PGP Desktop grundsätzlich, den SSL-Schutz zu aktivieren, **da bei einer durch SSL geschützten Verbindung nicht nur alle mit der PGP-Anwendung verschlüsselten Nachrichten zwischen E-Mail-Server und E-Mail-Client geschützt werden, sondern auch die Authentifizierungspassphrase des E-Mail-Servers, wenn sie an den E-Mail-Server gesendet wird.**

- **Wenn die Verbindung durch SSL geschützt ist:** Wenn im E-Mail-Client der SSL-Schutz für die Verbindung zum E-Mail-Server aktiviert wurde und PGP Desktop Ihre Nachrichten verschlüsseln oder entschlüsseln soll, müssen Sie den Schutz deaktivieren. PGP Desktop kann die Nachrichten nicht verarbeiten, wenn sie bereits mit SSL verschlüsselt sind.

  Wenn der SSL-Schutz im E-Mail-Client deaktiviert wurde, bedeutet dies nicht, dass Nachrichten, die nicht mit der PGP-Anwendung verschlüsselt wurden, bei der Übertragung vom und zum E-Mail-Server ungeschützt sind. Wie bei jeder Verbindung, die nicht durch SSL geschützt ist, versucht PGP Desktop automatisch, für diese Verbindung den SSL-Schutz zu aktivieren, wenn dieser vom E-Mail-Server unterstützt wird (falls Sie im Dialogfeld „Servereinstellungen“ für die SSL/TLS-Einstellung die Option **Automatisch** ausgewählt haben). Wenn der E-Mail-Server keine SSL-Verbindungen unterstützt, sendet PGP Desktop die Nachrichten während der Sitzung über eine ungeschützte Verbindung.

  Ihre Nachrichten werden nur dann als Klartext an den E-Mail-Server gesendet, wenn die Nachrichten nicht mit der PGP-Anwendung verschlüsselt sind und die Verbindung zum E-Mail-Server nicht durch SSL geschützt werden kann oder wenn Sie für die SSL/TLS-Einstellung die Option **Nicht versuchen** ausgewählt haben.

- **Wenn Nachrichten nicht als Klartext gesendet werden dürfen:** In einigen Sicherheitsrichtlinien ist festgelegt, dass nur geschützte und keine ungeschützten Nachrichten gesendet werden dürfen. Bei Bedarf können Sie PGP Desktop so konfigurieren, dass derartige Sicherheitsrichtlinien unterstützt werden.

  Wählen Sie den entsprechenden PGP Messaging-Dienst aus und öffnen Sie das Dialogfeld „Servereinstellungen“ (klicken Sie auf den Namen des Servers, der derzeit für den Dienst in den Kontoeigenschaften im Feld für den Server ausgewählt ist). Wählen Sie in der Liste „SSL/TLS“ eine *andere* Option als **Automatisch** aus.

Wenn diese Option aktiviert ist, wird das Senden und Empfangen von Nachrichten zwischen dem E-Mail-Server und PGP Desktop nur über eine durch SSL geschützte Verbindung abgewickelt. Falls keine durch SSL geschützte Verbindung hergestellt werden kann, kommuniziert PGP Desktop nicht mit dem Server.

Hinweis: Diese Option darf nur aktiviert werden, wenn Sie sicher sind, dass der E-Mail-Server das SSL-Protokoll unterstützt. Auf diese Weise wird sichergestellt, dass PGP Desktop keine Nachrichten über ungeschützte Verbindungen sendet oder empfängt, falls beispielsweise ein Problem bei der Aushandlung des SSL-Protokolls für die Verbindung auftritt. Wenn Sie diese Option aktivieren und der E-Mail-Server SSL nicht unterstützt, sendet oder empfängt PGP Desktop keine Nachrichten.

- **Wenn SSL im E-Mail-Client aktiviert sein soll:** Damit Sie PGP Desktop verwenden können, wenn SSL im E-Mail-Client aktiviert ist, müssen Sie die Option **Bei SSL/TLS-Verbindungsversuch durch E-Mail-Client warnen** für den Mailserver für eingehende Nachrichten, für den Postausgangsserver oder für beide Server deaktivieren. Wenn diese Option für eine Verbindung zu einem E-Mail-Server deaktiviert ist, ignoriert PGP Desktop den ein- und ausgehenden E-Mail-Verkehr über diese Verbindung, wenn die Verbindung durch SSL geschützt ist.

  PGP Desktop überwacht die Verbindungen zu und von diesem Server und ignoriert den E-Mail-Verkehr, der über Verbindungen gesendet oder empfangen wird, die durch SSL geschützt sind. Falls PGP Desktop jedoch eine Verbindung erkennt, die nicht durch SSL geschützt ist, wird der Verkehr wie alle anderen ungeschützten Verbindungen gehandhabt. Die Anwendung versucht, für diese Verbindung den SSL-Schutz zu aktivieren (wenn der Modus „Automatisch“ ausgewählt ist) und entsprechende Richtlinien auf die Nachrichten anzuwenden.

Schlüsselmodi

Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, arbeitet PGP Desktop in einem Schlüsselmodus.

Hinweis: Die Informationen in diesem Abschnitt gelten *nur* für Benutzer, die PGP Desktop in einer von einem PGP Universal Server geschützten E-Mail-Domäne einsetzen.

Folgende Schlüsselmodi sind verfügbar:

- **Server Key Mode (SKM):** Schlüssel werden auf dem PGP Universal Server erstellt und von diesem verwaltet. Sie werden ausschließlich bei Bedarf für den Computer freigegeben, auf dem Sie PGP Desktop ausführen. Ihr privater Schlüssel wird nur auf dem PGP Universal Server gespeichert, der auch die gesamte diesbezügliche Verwaltung übernimmt. Da der PGP Universal-Administrator vollständigen Zugriff auf Ihren privaten Schlüssel hat, kann er auf alle Nachrichten zugreifen, die Sie verschlüsseln. Dieser Schlüsselmodus ist *nicht* mit Smartcards kompatibel (Smartcards können nur unter Windows verwendet werden).

  Ab PGP Desktop Version 10.0 können SKM-Schlüssel, die zuvor nur für Messaging verwendet werden konnten, für alle anderen PGP Desktop-Verschlüsselungsvorgänge genutzt werden. Dies umfasst das Verschlüsseln von Laufwerken und Dateien und das Entschlüsseln von MAPI-E-Mail-Nachrichten im Offlinemodus.

  Wenn Sie einen SKM-Schlüssel verwenden, entfällt generell die Notwendigkeit, eine Passphrase zur Authentifizierung einzugeben. SKM-Schlüsselpassphrasen werden von PGP Desktop auf Zufallsbasis erzeugt und verschlüsselt gespeichert. Wenn PGP Desktop eine Passphrase erfordert, ruft PGP Desktop die verschlüsselte Passphrase vom System ab, ohne dass eine Aktion Ihrerseits erforderlich ist.

- **Client-Schlüsselmodus (CKM):** Schlüssel werden auf dem Computer erstellt und verwaltet, auf dem Sie PGP Desktop ausführen. Private Schlüssel werden nicht für den PGP Universal Server freigegeben. Auch alle kryptografischen Operationen (Verschlüsseln, Entschlüsseln, Signieren, Verifizieren) werden auf dem Computer durchgeführt, auf dem Sie PGP Desktop ausführen. Unter Windows ist dieser Schlüsselmodus mit Smartcards kompatibel.

- **Guarded Key Mode (GKM):** Dieser Modus ähnelt CKM, jedoch wird eine *verschlüsselte* Kopie des privaten Schlüssels auf dem PGP Universal Server gespeichert, auf den Sie über einen anderen Computer zugreifen können. Da der Schlüssel verschlüsselt ist, kann der PGP Universal-Administrator nicht darauf zugreifen und der Zugriff ist ausschließlich Ihnen vorbehalten. Dieser Schlüsselmodus ist mit Smartcards kompatibel (nur unter Windows), sofern der Schlüssel nicht direkt auf der Smartcard erstellt wird (d. h. der Schlüssel muss auf die Smartcard kopiert werden).

- **Server Client Key Mode (SCKM):** Dieser Modus ist ebenfalls mit CKM vergleichbar, jedoch wird eine Kopie des privaten *Verschlüsselungsschlüssel* auf dem PGP Universal Server gespeichert. Private *Signaturschlüssel* befinden sich grundsätzlich nur auf dem Computer, auf dem Sie PGP Desktop ausführen. Dieser Schlüsselmodus dient der Einhaltung von Gesetzen und Unternehmensrichtlinien, die verlangen, dass der Benutzer stets die Kontrolle über den privaten Signaturschlüssel behält, während der private Verschlüsselungsschlüssel gespeichert wird und in Notfällen zugänglich ist. Dieser Schlüsselmodus ist mit Smartcards kompatibel (nur unter Windows), sofern der Schlüssel nicht direkt auf der Smartcard erstellt wird. Für SCKM ist ein Schlüssel mit einem separaten Signatur-Unterschlüssel erforderlich, der mit PGP Desktop 9.5 oder höher für einen neuen Schlüssel erstellt oder mit PGP Desktop 9.5 oder höher einem älteren Schlüssel hinzugefügt werden kann.

Abhängig von der Konfiguration Ihrer Version von PGP Desktop durch den PGP-Administrator können Sie den Schlüsselmodus möglicherweise nicht auswählen. Von der Konfiguration hängt auch ab, ob Sie den Schlüsselmodus ändern können.

Wenden Sie sich an den PGP-Administrator, wenn Sie weitere Fragen zum Schlüsselmodus haben.

Schlüsselmodus ermitteln

Beachten Sie, dass nur PGP Desktop-Benutzer in einer mit PGP Universal geschützten Umgebung über einen Schlüsselmodus verfügen, nicht jedoch Benutzer eigenständiger Versionen von PGP Desktop.

So ermitteln Sie Ihren Schlüsselmodus

- Öffnen Sie PGP Desktop und wählen Sie den PGP Messaging-Dienst aus, dessen Schlüsselmodus Sie ermitteln möchten. Die Kontoeigenschaften und Sicherheitsrichtlinien für den ausgewählten Dienst werden angezeigt.

  Im Feld **Universal-Server** ist der Schlüsselmodus für den ausgewählten Dienst in Klammern hinter dem Namen des PGP Universal Servers angegeben (z. B. **keys.beispiel.com (GKM)**). Der Schlüsselmodus für den ausgewählten Dienst ist in diesem Beispiel also Guarded Key Mode (GKM) und der zugehörige PGP Universal Server ist keys.beispiel.com.

Schlüsselmodus ändern

Abhängig von der Konfiguration Ihrer Version von PGP Desktop durch den PGP-Administrator können Sie den Schlüsselmodus möglicherweise nicht ändern.

So ändern Sie den Schlüsselmodus

1. Öffnen Sie PGP Desktop und wählen Sie den PGP Messaging-Dienst aus, dessen Schlüsselmodus Sie ändern möchten. Die Kontoeigenschaften und Sicherheitsrichtlinien für den ausgewählten Dienst werden angezeigt.
2. Klicken Sie auf **Schlüsselmodus**. Der Bildschirm für den PGP Universal-Schlüsselmodus wird geöffnet und enthält Informationen zum aktuellen Schlüsselverwaltungsmodus.
3. Klicken Sie auf **Schlüssel zurücksetzen** und klicken Sie in der daraufhin angezeigten Bestätigungsmeldung auf **Ja**. Der Einrichtungsassistent für PGP-Schlüssel wird geöffnet.
4. Lesen Sie den angezeigten Text und klicken Sie auf **Weiter**. Der Bildschirm „Schlüsselverwaltung auswählen“ wird angezeigt.
5. Wählen Sie den gewünschten Schlüsselmodus aus. Abhängig von der Konfiguration Ihrer Kopie von PGP Desktop durch den PGP Universal-Administrator stehen Ihnen einige Schlüsselmodi möglicherweise nicht zur Verfügung.
6. Klicken Sie auf **Weiter**. Der Bildschirm „Schlüsselquelle auswählen“ wird angezeigt.
7. Wählen Sie eine der folgenden Optionen aus:
   - **Neuer Schlüssel**: Sie werden aufgefordert, einen neuen PGP-Schlüssel zu erstellen, der zum Schutz des Messaging-Verkehrs verwendet wird.
   - **PGP Desktop-Schlüssel**: Sie werden aufgefordert, einen vorhandenen PGP-Schlüssel anzugeben, der zum Schutz des Messaging-Verkehrs verwendet wird.
   - **Schlüssel importieren**: Sie werden aufgefordert, einen PGP-Schlüssel zu importieren, der zum Schutz des Messaging-Verkehrs verwendet wird.
8. Wählen Sie die gewünschte Option aus und klicken Sie auf **Weiter**.
9. Wenn Sie **Neuer Schlüssel** ausgewählt haben, führen Sie folgende Schritte aus:
   - Geben Sie eine Passphrase für den Schlüssel ein und klicken Sie auf **Weiter**.
   - Wenn der Schlüssel erstellt wurde, klicken Sie auf **Weiter**.
   - Klicken Sie auf **Beenden**.
10. Wenn Sie **PGP Desktop-Schlüssel** ausgewählt haben, führen Sie folgende Schritte aus:
    - Wählen Sie den gewünschten Schlüssel auf dem lokalen Schlüsselbund aus und klicken Sie auf **Weiter**.
    - Klicken Sie auf **Beenden**.

11 Wenn Sie **Schlüssel importieren** ausgewählt haben, führen Sie folgende Schritte aus:

- Wechseln Sie zu der Datei mit dem PGP-Schlüssel, den Sie importieren möchten (Datei muss einen privaten Schlüssel enthalten). Klicken Sie dann auf **Weiter**.
- Klicken Sie auf **Beenden**.

Tipp: Sie können den Schlüsselmodus auch in den PGP-Optionen ändern. Wählen Sie **Extras > PGP-Optionen** und klicken Sie auf die Registerkarte „Erweitert". Klicken Sie auf **Schlüssel zurücksetzen** und führen Sie die oben angegebenen Schritte aus, wenn der Einrichtungsassistent für PGP-Schlüssel angezeigt wird. Diese Option ist verfügbar, wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen.

PGP-Protokoll anzeigen

Im PGP-Protokoll werden die Aktionen angezeigt, die von PGP Desktop zum Schutz Ihrer Nachrichten ergriffen werden.

So zeigen Sie das Protokoll von PGP Desktop an

1 Damit Protokolle angezeigt werden können, müssen Sie die Protokollfunktion aktivieren. Klicken Sie dazu in PGP Desktop auf **Extras > PGP-Protokollierung**.

2 Klicken Sie in PGP Desktop auf das Bedienfeld „PGP Messaging" und wählen Sie **PGP-Protokoll** aus. Daraufhin wird das PGP-Protokoll im Anwendungsfenster angezeigt.

3 Führen Sie folgende Schritte aus, um die Anzeigeoptionen zu ändern oder Filter für bestimmte Protokollinformationen zu verwenden:

- Klicken Sie auf den Pfeil für das Menü **Protokoll anzeigen für**, um den Zeitraum auszuwählen, für den Protokolle angezeigt werden sollen.
- Klicken Sie auf den Pfeil für das Menü **Thema anzeigen**, um die Arten der Protokolle auszuwählen, die Sie anzeigen möchten. Sie haben die Wahl zwischen **Alle**, **PGP**, **E-Mail**, **IM**, **Whole Disk**, **NetShare**, **Zip/SDA** und **Virtual Disk**.
- Klicken Sie auf den Pfeil für das Menü **Stufe anzeigen**, um den Mindestschweregrad der Protokolleinträge auszuwählen, die Sie anzeigen möchten. Sie haben die Wahl zwischen **Fehler**, **Warnung**, **Info** und **Ausführlich**. Beachten Sie, dass die Option **Ausführlich** zu sehr großen Protokolldateien führen kann.

4 Nach Abschluss der Anzeige des Protokolls:

- Klicken Sie auf **Speichern**, um eine Kopie des PGP-Protokolls zu speichern.
- Klicken Sie auf **Sicher löschen**, wenn Sie die Einträge im PGP-Protokoll entfernen möchten.

8 Instant Messaging-Sitzungen sichern

In diesem Abschnitt finden Sie Informationen zum Sichern von Instant Messaging-Sitzungen (IM) mit PGP Desktop. Informationen zu PGP-Optionen für IM-Sitzungen finden Sie unter *Messaging-Optionen* (auf Seite 334).

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung verwenden, hat Ihr PGP Universal Server-Administrator ggf. bestimmte Funktionen deaktiviert. Ist eine Funktion deaktiviert, wird das Bedienelement auf der linken Seite nicht angezeigt und das Menü oder andere auf diese Funktion zutreffenden Optionen sind nicht verfügbar. Die in diesem Handbuch enthaltenen Abbildungen entsprechen der Standardinstallation, bei der alle Funktionen aktiviert sind. Wenn Ihr PGP Universal Server-Administrator diese Funktion deaktiviert hat, ist dieser Abschnitt für Sie nicht relevant.

In diesem Kapitel

Informationen zur Instant Messaging-Kompatibilität von PGP Desktop 143
Informationen zu den für die Verschlüsselung verwendeten Schlüsseln145
IM-Sitzungen verschlüsseln 145

Informationen zur Instant Messaging-Kompatibilität von PGP Desktop

PGP Desktop verschlüsselt automatisch standardmäßige AOL- und iChat-IM-Sitzungen, Direktverbindungen und Dateiübertragungen, wenn folgende Bedingungen erfüllt sind:

- Auf dem System beider Teilnehmer, auf dem die IM-Anwendung verwendet wird, ist PGP Desktop 9.0 oder höher installiert und wird ausgeführt. Wenn Sie bestätigen möchten, dass Sie PGP Desktop 9.0 oder höher verwenden, klicken Sie auf das PGP-Symbol im Infobereich der Taskleiste und wählen Sie im Kontextmenü die Option **Info über PGP** aus. (Wählen Sie im Fenster von PGP Desktop die Option **Hilfe > Info über PGP** aus.)
- Beide Teilnehmer haben die Option **zum Verschlüsseln von Instant Messages aktiviert. Führen Sie dazu folgende Schritte aus:**

- Wählen Sie unter Windows die Option **Extras > Optionen**, klicken Sie auf die Registerkarte „Messaging“ und aktivieren Sie das Kontrollkästchen **AOL Instant Messaging-Nachrichten (AIM) verschlüsseln**.
- Wählen Sie unter Mac OS X die Option **PGP > Einstellungen** aus, klicken Sie auf das Symbol „Messaging“ und aktivieren Sie das Kontrollkästchen **AOL Instant Messaging-Nachrichten (AIM) verschlüsseln**.

Tipp: Unter Windows können Sie schnell bestätigen, dass die Instant Messaging-Verschlüsselung aktiviert ist, indem Sie auf das PGP-Symbol im Infobereich der Taskleiste klicken. Im Kontextmenü sollte neben der Option **AIM-Proxy verwenden** ein Häkchen angezeigt werden.

- Beide Benutzer verwenden kompatible IM-Clients. Informationen zu kompatiblen IM-Clients finden Sie im folgenden Abschnitt.
- Die AIM-Adresse des Initiators der IM-Sitzung **ist** in der Buddy-Liste des Empfängers der Sitzung aufgeführt (andernfalls wird die Sitzung nicht verschlüsselt).

Die sichere IM-Funktion ist mit allen IM-Clients kompatibel, die das OSCAR-Protokoll für Instant Messaging von AOL unterstützen, z. B. AOL Instant Messenger, Trillian Pro, iChat und Gaim.

Für die Sitzungen für Dateiübertragung und Direktverbindung sind aktuelle Versionen dieser Clients erforderlich, damit sie von PGP Desktop verschlüsselt werden können. Darüber hinaus empfiehlt die PGP Corporation, beide Verbindungen (Direct IM/Direct Message und Dateiübertragung) so zu konfigurieren, dass der AOL-Proxy verwendet wird und der Buddy nicht direkt mit Ihrem Computer verbunden ist.

Hinweise:

Audio- und Videoverbindungen werden von PGP Desktop nicht verschlüsselt.

Die sichere IM-Funktion von PGP Desktop setzt zur Erhöhung der Sicherheit PFS (Perfect Forward Secrecy) ein. Alle zur Sicherung der IM-Sitzungen verwendeten Schlüssel werden zu Beginn der Verbindung erstellt und bei Trennung der Verbindung vernichtet. Für jede IM-Sitzung werden vollkommen neue Schlüsselsätze verwendet. Die Sicherheitsstufe von IM-Sitzungen wird dadurch zusätzlich erhöht.

Kompatibilität mit Instant Messaging-Clients

PGP Desktop ist bei der Verschlüsselung von AIM-Nachrichten, -Dateiübertragungen und -Direktverbindungen mit den folgenden Instant Messaging-Clients (kurz: IM-Clients) kompatibel:

- AOL AIM 6.5.5

- Wenn Sie Instant Message-Nachrichten mit AIM 6.5 verschlüsseln möchten, muss der von AIM verwendete Standard-Port von 493 auf 5190 gesetzt werden.
- Audio- und Videoverbindungen werden von PGP Desktop nicht verschlüsselt.
- Die Interoperabilität mit dem AIM-Dienst kann durch Änderungen an den eigentlichen AIM-Protokollen beeinträchtigt werden, die nach der Veröffentlichung von PGP Desktop Version 10.0 durchgeführt werden.

- Trillian 3.1 (Basic und Pro)

Andere IM-Clients können möglicherweise für einfaches Instant Messaging verwendet werden, wurden jedoch für die Verwendung nicht zertifiziert.

Informationen zu den für die Verschlüsselung verwendeten Schlüsseln

Jedes Mal, wenn Sie sich bei der IM-Software anmelden, wird ein RSA-Schlüssel mit 1024 Bit erstellt. Wenn Sie sich abmelden, wird dieser Schlüssel vernichtet. Dieser Schlüssel wird verwendet, um auf Zufallsbasis erzeugte Seed-Daten mit jedem Kommunikationspartner auszutauschen. Die Seed-Daten werden kombiniert und ein Hash wird angewendet, damit jeder Kommunikationsteilnehmer einen Satz symmetrischer Schlüssel erstellen kann, der für diese bestimmte Kommunikation verwendet wird (ein Schlüssel pro Richtung). Mit den symmetrischen Schlüsseln werden alle Nachrichten mit AES-256 verschlüsselt.

Ein Teil dieser Daten wird auch genutzt, um einen HMAC (Keyed-Hash Message Authentication Code) für jede Nachricht zu erstellen, damit die Integrität der Nachricht geprüft werden kann.

Hinweis: Die für sichere IM-Kommunikation verwendeten Schlüssel können nicht vom Benutzer konfiguriert werden.

IM-Sitzungen verschlüsseln

Wenn die in *Informationen zur Instant Messaging-Kompatibilität von PGP Desktop* (auf Seite 143) beschriebenen Bedingungen erfüllt sind, beginnen Sie Ihre IM-Sitzung ganz normal. IM-Sitzungen mit anderen PGP Desktop-Benutzern, die einen kompatiblen IM-Client verwenden, werden automatisch und transparent geschützt.

Es gibt verschiedene Methoden, um zu überprüfen, ob die IM-Sitzung geschützt ist:

- Beim Start einer IM-Sitzung wird eine Benachrichtigung von PGP Notifier angezeigt, dass eine gesicherte IM-Sitzung gestartet wurde.
- Wenn die IM-Sitzung beginnt, wird unterhalb der ersten Nachricht des anderen Benutzers der Sitzung zusätzlicher Text angezeigt, dass eine mit PGP Desktop verschlüsselte Konversation begonnen hat.
- Ein Schlosssymbol neben den Namen in der Buddy-Liste zeigt an, dass die Benutzer wahrscheinlich PGP Desktop verwenden, um ihre IM-Sitzungen zu sichern.

  Das Schlosssymbol könnte jedoch auch bedeuten, dass der Benutzer den integrierten AIM-Schutz verwendet.
- Wenn Sie das PGP-Protokoll nach dem Starten der IM-Sitzung öffnen, wird in einem Eintrag angegeben, dass die IM-Sitzung verschlüsselt ist. Beispiel:

  ```
  17:01:06 Info    Die mit PGP Desktop verschlüsselte AIM-
  Sitzung mit breynolds wird initialisiert. Hierbei wird
  Ihr Schlüssel mit der ID 0xEFDDCE3C verwendet.
  ```

9 E-Mail-Nachrichten mit PGP Viewer anzeigen

In diesem Abschnitt finden Sie Informationen zum Verwenden von PGP Viewer zum Entschlüsseln, Verifizieren und Anzeigen von entschlüsselten Nachrichten.

Hinweis: PGP Viewer wird nur auf Systemen ausgeführt, auf denen PGP Desktop installiert ist. PGP Viewer kann nicht als eigenständige Anwendung verwendet werden.

In diesem Kapitel

Übersicht über PGP Viewer 147
Verschlüsselte E-Mail-Nachrichten oder Dateien öffnen 149
E-Mail-Nachrichten in den Posteingang kopieren 150
E-Mail-Nachrichten exportieren 151
Zusätzliche Optionen angeben 151
Optionen in PGP Viewer festlegen 151
Sicherheitsfunktionen in PGP Viewer 152

Übersicht über PGP Viewer

Bei normaler Verwendung befindet sich PGP Desktop zwischen dem E-Mail-Client (z. B. Mozilla Thunderbird) und dem E-Mail-Server, um ausgehende Nachrichten zu verschlüsseln und zu signieren und eingehende Nachrichten zu entschlüsseln und zu verifizieren. Bei dieser Funktionsweise wird PGP Desktop „im E-Mail-Strom“ eingesetzt.

Mit PGP Viewer können Sie Nachrichten *außerhalb* des E-Mail-Stroms entschlüsseln, verifizieren und anzeigen.

Es gibt verschiedene Gründe, warum Sie verschlüsselte Nachrichten ggf. außerhalb des E-Mail-Stroms erhalten haben:

- **Sicher gespeicherte verschlüsselte Nachrichten:** Viele Organisationen speichern Nachrichten aus Sicherheitsgründen verschlüsselt. Durch das Speichern befinden sie sich außerhalb des E-Mail-Stroms, jedoch können sie von PGP Viewer entschlüsselt, verifiziert und angezeigt werden, wobei die ursprüngliche verschlüsselte Nachricht beibehalten wird.

- **Verschlüsselter Text in einer Webmail-Nachricht:** An ein Webmail-Konto gesendete verschlüsselte Nachrichten können von PGP Desktop nicht entschlüsselt werden. Diese Nachrichten können jedoch von PGP Viewer entschlüsselt werden. Öffnen Sie die Dateianlage message.pgp mit PGP Viewer.
- **Verschlüsselter Text, der nicht von PGP Desktop entschlüsselt wurde:** Wenn eine Nachricht vom E-Mail-Client automatisch heruntergeladen wurde, als PGP Desktop nicht ausgeführt wurde oder Ihre Passphrase nicht zwischengespeichert war, erhalten Sie möglicherweise verschlüsselten Nachrichtentext außerhalb des E-Mail-Stroms.

Mit PGP Viewer können verschiedene Arten von Messaging-Inhalt entschlüsselt, verifiziert und angezeigt werden:

- Aktueller mit einer PGP-Anwendung verschlüsselter Inhalt (PGP/MIME und PGP-partitioniert)
- Älterer mit einer PGP-Anwendung verschlüsselter Inhalt (PGP/MIME und PGP-partitioniert)
- Mit RFC-2822 kompatibler verschlüsselter Inhalt

PGP Viewer verwendet Schlüsselbunde von PGP Desktop für Vorgänge, die Schlüssel erfordern.

PGP Viewer behält entsprechende Einstellungen von PGP Desktop bei, z. B. Optionen zum Zwischenspeichern von Passphrasen.

In einer von einem PGP Universal Server verwalteten Umgebung sucht PGP Viewer anhand der jeweiligen Richtlinie nach Verifizierungsschlüsseln.

PGP Viewer zeigt Signaturinformationen für Nachrichten, die von PGP Viewer entschlüsselt wurden, im Nachrichtenfenster und nicht in der eigentlichen Nachricht an. Dadurch wird der Zugriff auf vollständige Signaturinformationen ermöglicht und das Spoofing von Inline-Signaturanmerkungen verhindert.

Kompatible E-Mail-Clients

Mit PGP Viewer können Sie den Text einer entschlüsselten/verifizierten Nachricht in die folgenden E-Mail-Clients kopieren:

- Windows Mail (Windows)
- Microsoft Outlook (Windows)
- Thunderbird (Windows und Mac OS X)
- Outlook Express (Windows)
- Mail.app (Mac OS X)

Aufgrund des Designs der Architektur von Lotus Notes kann eine verschlüsselte Nachricht nicht zum Entschlüsseln aus dem Lotus Notes-E-Mail-Client in PGP Viewer gezogen werden.

Verschlüsselte E-Mail-Nachrichten oder Dateien öffnen

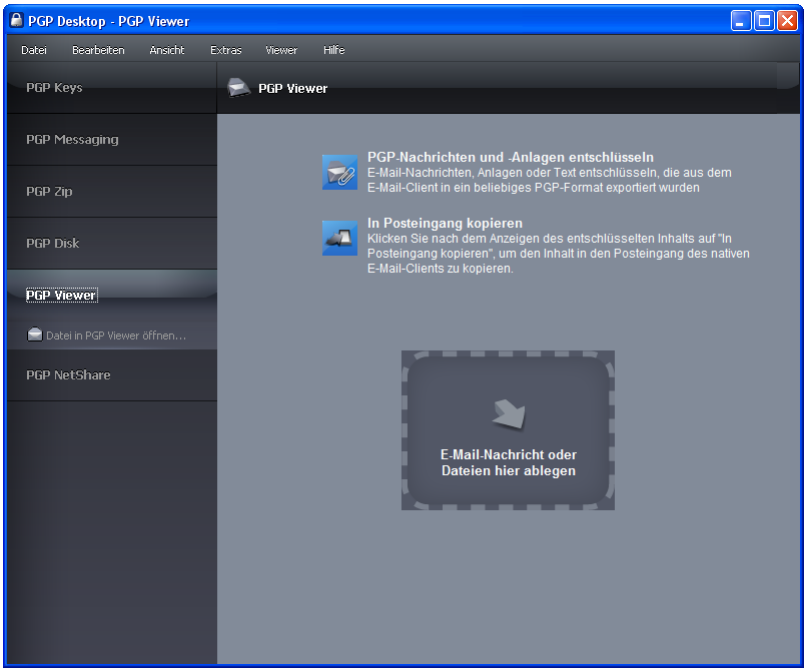
Mit PGP Viewer können Sie folgende Arten von verschlüsselten Nachrichtendateien öffnen (entschlüsseln, verifizieren und anzeigen):

- ***.pgp:** Wurde mit einer PGP-Anwendung erstellt.
- ***.eml**: Wurde mit Outlook Express oder Thunderbird erstellt.
- ***.emlx**: Wurde unter Mac OS X mit dem E-Mail-Programm mail.app von Apple erstellt.
- ***.msg**: Wurde mit Microsoft Outlook erstellt.

Wenn PGP Viewer eine verschlüsselte Nachricht öffnet, wird der verschlüsselte Text nicht überschrieben. Die Originalnachricht bleibt erhalten.

So können Sie eine verschlüsselte Nachricht aus einer Datei entschlüsseln, verifizieren und anzeigen

1 Öffnen Sie PGP Viewer. Klicken Sie hierzu auf das PGP-Symbol in der Taskleiste und wählen Sie „PGP Viewer“ aus. Sie können auch in PGP Desktop das Bedienfeld „PGP Viewer“ auswählen.


PGP Desktop - PGP Viewer
Datei
Bearbeiten
Ansicht
Extras
Viewer
Hilfe
PGP Keys
PGP Messaging
PGP Zip
PGP Disk
PGP Viewer
Datei in PGP Viewer öffnen...
PGP NetShare
PGP Viewer
PGP-Nachrichten und -Anlagen entschlüsseln
E-Mail-Nachrichten, Anlagen oder Text entschlüsseln, die aus dem E-Mail-Client in ein beliebiges PGP-Format exportiert wurden
In Posteingang kopieren
Klicken Sie nach dem Anzeigen des entschlüsselten Inhalts auf "In Posteingang kopieren", um den Inhalt in den Posteingang des nativen E-Mail-Clients zu kopieren.
E-Mail-Nachricht oder Dateien hier ablegen

2 Klicken Sie auf **Datei in PGP Viewer öffnen** oder öffnen Sie das Menü **Viewer** und wählen Sie **Datei in PGP Viewer öffnen** aus.

Das Dialogfeld **Nachrichtendatei öffnen** wird angezeigt.

3 Wechseln Sie im Dialogfeld „Nachrichtendatei öffnen“ zur gewünschten Datei, wählen Sie sie aus und klicken Sie auf **Öffnen**. Die Nachricht wird von PGP Viewer in einem separaten Fenster entschlüsselt, verifiziert und angezeigt.

Tipp: Sie können die Datei, die Sie öffnen möchten, in den Teil des PGP Viewer-Fensters ziehen, in dem Folgendes angezeigt wird: **E-Mail-Nachricht oder Dateien hier ablegen**. PGP Viewer öffnet die Datei, entschlüsselt und verifiziert sie und zeigt die Nachricht an.

4 Wenn Sie eine andere Nachricht öffnen möchten, klicken Sie in der Symbolleiste auf **Nachricht öffnen**, wechseln Sie zur gewünschten Datei, wählen Sie sie aus und klicken Sie auf **Öffnen**. PGP Viewer entschlüsselt und verifiziert die Nachricht und zeigt sie an. Auf der linken Seite des PGP Viewer-Bildschirms wird ein Bereich angezeigt, in dem Sie alle geöffneten Nachrichten sehen können.

5 Klicken Sie zum Öffnen oder Schließen eines Bereichs auf der linken Seite des PGP Viewer-Bildschirms in der Symbolleiste auf die Schaltfläche „Fenster“.

E-Mail-Nachrichten in den Posteingang kopieren

Mit PGP Viewer können Sie die Klartextversionen von entschlüsselten Nachrichten in den Posteingang des E-Mail-Clients kopieren.

So kopieren Sie eine Nachricht in den Posteingang des E-Mail-Clients

1 Wenn die Nachricht im Fenster von PGP Viewer angezeigt wird, klicken Sie auf **In Posteingang kopieren**. Im Bestätigungsdialogfeld „In Posteingang kopieren“ wird der Name des E-Mail-Clients angezeigt, auf den die Nachricht kopiert wird. Informationen zum Ändern dieser Einstellung finden Sie unter *Optionen in PGP Viewer festlegen* (auf Seite 151).

2 Klicken Sie auf **OK**, um fortzufahren.

Wenn Sie zum ersten Mal eine Nachricht in den E-Mail-Client Mozilla Thunderbird kopieren, werden Sie aufgefordert, ein Add-On zu installieren.

Klicken Sie auf **Ja**, um das Add-On zu installieren, und folgen Sie den Anweisungen auf dem Bildschirm oder klicken Sie auf **Nein**. Sie müssen Thunderbird 2.0 oder höher verwenden, um das Add-On installieren zu können.

3 PGP Viewer öffnet den E-Mail-Client und kopiert eine Klartextversion der Nachricht in den Posteingang.

E-Mail-Nachrichten exportieren

Verwenden Sie PGP Viewer, um eine entschlüsselte Nachricht in eine Datei zu exportieren.

So exportieren Sie eine Nachricht von PGP Viewer in eine Datei

1. Wenn die Nachricht im Fenster von PGP Viewer angezeigt wird, klicken Sie auf **Exportieren**. Das Dialogfeld „Nachrichtendatei exportieren“ wird angezeigt.
2. Geben Sie im Dialogfeld „Nachrichtendatei exportieren“ den gewünschten Speicherort, den Dateinamen und das Format für die Datei an. Klicken Sie dann auf **Speichern**. PGP Viewer speichert die Datei am angegebenen Speicherort.

Zusätzliche Optionen angeben

Verwenden Sie auf der Symbolleiste von PGP Viewer die Schaltfläche „Extras“ (rechts außen), um mehrere Funktionen von PGP Viewer festzulegen:

- **Textcodierung**: Geben Sie das Textcodierungsformat für die Nachricht an, die gegenwärtig von PGP Viewer angezeigt wird.
- **Remotebilder anzeigen**: Zeigen Sie die externen Ressourcen (Bilder, Cascading Stylesheets (CSS), iframe-Inhalte usw.) für die Nachricht an, die derzeit von PGP Viewer angezeigt wird. In den Einstellungen können Sie festlegen, dass die externen Ressourcen von PGP Viewer automatisch angezeigt werden sollen.
- **Nachrichtenquelle anzeigen**: Zeigen Sie die Quelle der Nachricht an, die derzeit von PGP Viewer angezeigt wird. Die Nachrichtenquelle kann weitere Informationen zur Nachricht enthalten.
- **Einstellungen**: Zeigen Sie das Dialogfeld „Einstellungen“ von PGP Viewer an.

Optionen in PGP Viewer festlegen

PGP Viewer umfasst Optionen (Einstellungen), über die bestimmte Funktionen gesteuert werden können.

So greifen Sie auf die Einstellungen von PGP Viewer zu

1. Öffnen Sie PGP Viewer über den PGP-Infobereich der Taskleiste oder verwenden Sie PGP Viewer zum Entschlüsseln, Verifizieren und Anzeigen einer Nachricht.

   Der Bildschirm „PGP Viewer“ wird angezeigt.

2. Klicken Sie auf das Symbol „Extras“ (ganz rechts in der Symbolleiste von PGP Viewer) und wählen Sie die Option **Einstellungen** aus. Das Dialogfeld „Einstellungen“ wird angezeigt.

3. Klicken Sie auf die Registerkarte „Allgemein“ und legen Sie folgende Optionen fest:

   - **Benutzer muss Befehl „In Posteingang kopieren“ bestätigen**: Steuert, ob beim Kopieren von Text aus PGP Viewer in den Posteingang des E-Mail-Clients eine Aufforderung zur Bestätigung angezeigt wird. Die Einstellung ist standardmäßig aktiviert.
   - **Remotebilder automatisch laden**: Steuert, ob externe Ressourcen wie Bilder, CSS-Stylesheets oder iframe-Inhalt automatisch von PGP Viewer geladen werden. Die Einstellung ist standardmäßig deaktiviert, da dies ein Sicherheitsrisiko darstellen kann.
   - **E-Mail-Client verwenden**: Hier können Sie den E-Mail-Client angeben, in den PGP Viewer Inhalt kopiert. Die Standardeinstellung ist **Windows-Standard (E-Mail)**. PGP Viewer ermittelt den standardmäßigen Windows-E-Mail-Client und verwendet diesen als Standard. Sie können auch **Outlook**, **Outlook Express** und **Thunderbird** auswählen.

4. Wählen Sie die Registerkarte „Text“ aus und legen Sie folgende Optionen fest:

   - **Schriftart**: Legt die Schriftart fest, die PGP Viewer zum Anzeigen von Text verwendet.
   - **Textfarbe**: Legt die Farbe fest, in der PGP Viewer Text anzeigt.
   - **Hintergrundfarbe**: Legt die Hintergrundfarbe von Text fest, die PGP Viewer anzeigt.

Sicherheitsfunktionen in PGP Viewer

PGP Viewer gewährleistet Ihre Sicherheit proaktiv:

- Für den in PGP Viewer eingebetteten Webbrowser, der Messaging-Inhalt anzeigt, sind JavaScript, Java-Applets und Plug-ins deaktiviert. Dadurch wird verhindert, dass ein Angreifer böswillige Nutzlast übermittelt, die von PGP Viewer andernfalls geladen würde.

- Externe Ressourcen wie Bilder, CSS-Stylesheets oder iframe-Inhalt (ein Inline-Frame, der ein anderes Dokument enthält) werden entsprechend der Einstellung **Remotebilder automatisch laden** automatisch geladen. Aus Sicherheitsgründen ist diese Einstellung standardmäßig deaktiviert. Wenn diese Einstellung deaktiviert ist, generiert PGP Viewer keinen Netzwerkverkehr zu externen Websites.

10 Laufwerke mit PGP Whole Disk Encryption schützen

PGP Whole Disk Encryption (PGP WDE) sperrt den gesamten Inhalt von Desktop- oder Laptop-Computern, externen Laufwerken und USB-Flash-Laufwerken, einschließlich Startsektoren, System- und Auslagerungsdateien. Sie können PGP Whole Disk Encryption auch verwenden, um ausschließlich die Startpartition oder Windows-Partitionen zu verschlüsseln. Die Verschlüsselung läuft für den Benutzer transparent im Hintergrund ab. Wichtige Daten werden automatisch geschützt, ohne dass weitere Eingriffe erforderlich sind.

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung verwenden, hat Ihr PGP Universal Server-Administrator ggf. bestimmte Funktionen deaktiviert. Ist eine Funktion deaktiviert, wird das Bedienelement auf der linken Seite nicht angezeigt und das Menü oder andere auf diese Funktion zutreffenden Optionen sind nicht verfügbar. Die in diesem Handbuch enthaltenen Abbildungen entsprechen der Standardinstallation, bei der alle Funktionen aktiviert sind. Wenn Ihr PGP Universal Server-Administrator diese Funktion deaktiviert hat, ist dieser Abschnitt für Sie nicht relevant.

Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, hat der PGP-Administrator möglicherweise per Richtlinie festgelegt, dass alle Startlaufwerke verschlüsselt sein müssen. In diesem Fall überprüft PGP Desktop in regelmäßigen Abständen, ob die Laufwerke verschlüsselt sind, und setzt die Richtlinie durch das automatische Verschlüsseln nicht verschlüsselter Startlaufwerke durch.

Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, hat der PGP-Administrator möglicherweise den PGP Whole Disk Encryption BootGuard-Bildschirm angepasst, damit zusätzlicher Text oder ein eigenes Bild, z. B. das Logo der Organisation, angezeigt wird. Die in diesem Handbuch enthaltenen Abbildungen entsprechen der Standardinstallation. Der Ihnen angezeigte Anmeldebildschirm sieht möglicherweise anders aus, wenn er vom Administrator angepasst wurde.

In diesem Kapitel

Informationen zu PGP Whole Disk Encryption 156
PGP Whole Disk Encryption lizenzieren 158
Laufwerk auf die Verschlüsselung vorbereiten 159
Authentifizierungsmethode für das Laufwerk bestimmen 167
Verschlüsselungsoptionen festlegen 170
Laufwerke oder Partitionen verschlüsseln 177
Mit PGP Whole Disk Encryption verschlüsselte Laufwerke verwenden 184
Einzelanmeldung mit PGP Whole Disk Encryption verwenden 190
Schutz von Laufwerken aufrechterhalten 194
Mit Wechseldatenträgern arbeiten 203
PGP Whole Disk Encryption in einer von einem PGP Universal Server verwalteten Umgebung verwenden 206
Daten von verschlüsselten Laufwerken wiederherstellen 209
Mit PGP Whole Disk Encryption verschlüsselte Laufwerke entschlüsseln 212
Spezielle Sicherheitsmaßnahmen von PGP Desktop 213
Windows-Vorinstallationsumgebung verwenden 215

Informationen zu PGP Whole Disk Encryption

Wenn Sie ein ganzes Laufwerk mit PGP Whole Disk Encryption verschlüsseln, wird jeder Sektor mit einem symmetrischen Schlüssel verschlüsselt. Dies umfasst alle Dateien, einschließlich Betriebssystemdateien, Programmdateien, Datendateien, Auslagerungsdateien, freien Speicherplatz sowie temporäre Dateien.

Bei jedem nachfolgenden Systemstart werden Sie von PGP Whole Disk Encryption zur Eingabe der richtigen Passphrase aufgefordert. Die verschlüsselten Daten werden daraufhin entschlüsselt, wenn Sie auf sie zugreifen. Bevor Daten auf das Laufwerk geschrieben werden, verschlüsselt PGP Whole Disk Encryption diese Daten. Solange Sie für das mit PGP Whole Disk Encryption verschlüsselte Laufwerk authentifiziert sind (nach Eingabe der korrekten Passphrase im PGP BootGuard-Bildschirm), sind die Dateien verfügbar. Wenn Sie das System herunterfahren, ist das Laufwerk vor Verwendung durch andere Personen geschützt.

Es ist wichtig, dass Sie sich vor der Verschlüsselung des Laufwerks mit PGP Whole Disk Encryption bewusst sind, wie ein mit PGP Whole Disk Encryption verschlüsseltes Laufwerk erstellt und verwendet wird:

1. Stellen Sie sicher, dass die PGP Desktop-Lizenz die Verwendung der Funktion unterstützt (siehe *PGP Whole Disk Encryption lizenzieren* (auf Seite 158)).
2. Führen Sie die Schritte unter *Laufwerk auf die Verschlüsselung vorbereiten* (auf Seite 159) aus.
3. Wählen Sie die Authentifizierungsmethode zum Verschlüsseln des Laufwerks aus (siehe *Authentifizierungsmethode für das Laufwerk bestimmen* (auf Seite 167)).
4. Wählen Sie die zu verwendenden Verschlüsselungsoptionen aus (siehe *Verschlüsselungsoptionen festlegen* (auf Seite 170)).
5. Starten Sie den Verschlüsselungsprozess (siehe *Laufwerke oder Partitionen verschlüsseln* (auf Seite 177)).
6. Machen Sie sich mit der Verwendung eines verschlüsselten Laufwerks vertraut (siehe *Mit PGP Whole Disk Encryption verschlüsselte Laufwerke verwenden* (auf Seite 184)).
7. Machen Sie sich mit der Wartung des verschlüsselten Laufwerks vertraut (siehe *Schutz von Laufwerken aufrechterhalten* (auf Seite 194)).
8. Machen Sie sich damit vertraut, wie Sie das Laufwerk bei Bedarf entschlüsseln (siehe *Mit PGP Whole Disk Encryption verschlüsselte Laufwerke entschlüsseln* (auf Seite 212))
9. Machen Sie sich mit den Funktionen vertraut, mit denen Sie Sicherheitsprobleme vermeiden können (siehe Spezielle Sicherheitsmaßnahmen von PGP Desktop).

Wenn Sie ein PGP Universal-Administrator sind oder PGP Whole Disk Encryption in einer von einem PGP Universal Server verwalteten Umgebung verwenden, finden Sie weitere Informationen unter *PGP Whole Disk Encryption in einer von einem PGP Universal Server verwalteten Umgebung verwenden* (auf Seite 206).

Warnung: Nachdem Sie ein Laufwerk entsperrt haben, stehen die darauf befindlichen Dateien nicht nur Ihnen, sondern allen Personen zur Verfügung, die physischen Zugang zu dem System haben. Die Dateien bleiben so lange entsperrt, bis Sie den Computer herunterfahren und die Dateien dadurch wieder sperren. Verwenden Sie ein PGP Virtual Disk-Laufwerk für Dateien, die auch dann geschützt bleiben sollen, wenn Sie am Computer arbeiten. Weitere Informationen finden Sie unter *PGP Virtual Disk-Laufwerke verwenden* (auf Seite 219).

Worin unterscheidet sich PGP Whole Disk Encryption von PGP Virtual Disk?

Der Unterschied zwischen PGP Virtual Disk und PGP Whole Disk Encryption liegt darin, dass sich PGP Virtual Disk-Laufwerke wie zusätzliche Laufwerke im System verhalten, die auch dann gesperrt werden können, wenn Sie am Computer arbeiten. Diese Laufwerke sind mit einem Tresor vergleichbar, in dem Dateien aufbewahrt werden, die geschützt werden müssen. Es handelt sich dabei nicht um ein physisches, sondern um ein virtuelles Laufwerk, das mit PGP Virtual Disk erstellt und verwaltet wird.

PGP Whole Disk Encryption schützt die gesamte physische Festplatte.

Beide Produkte arbeiten unabhängig voneinander und können daher gleichzeitig eingesetzt werden. Weitere Informationen finden Sie unter *PGP Virtual Disk-Laufwerke verwenden* (auf Seite 219).

PGP Whole Disk Encryption lizenzieren

Damit Sie PGP Whole Disk Encryption verwenden können, muss Ihre Kopie von PGP Desktop über eine Lizenz verfügen, die diese Funktion unterstützt.

So überprüfen Sie, ob die Lizenz PGP Whole Disk Encryption unterstützt

1. Öffnen Sie PGP Desktop.
2. Wählen Sie **Hilfe > Lizenz** aus. Das Dialogfeld für die PGP Desktop-Lizenz wird angezeigt.
3. Suchen Sie unter **Produktinformationen** das Symbol **PGP Whole Disk Encryption**. Zeigen Sie mit der Maus auf den Produktnamen, um Informationen zum Produkt anzuzeigen und zu erfahren, ob Sie derzeit über eine gültige Nutzungslizenz verfügen.

Wenn PGP Whole Disk Encryption von der Lizenz nicht unterstützt wird, können Sie mit einem der folgenden Verfahren weitere Informationen zur Lizenzierung von PGP Desktop abrufen:

- Falls Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung verwenden, erhalten Sie Informationen zur Unterstützung von PGP Whole Disk Encryption im Rahmen Ihrer Lizenz vom PGP-Administrator. Weitere Informationen finden Sie unter *PGP Desktop mit PGP Universal Server verwenden* (auf Seite 357).
- Falls Sie PGP Desktop nicht in einer von einem PGP Universal Server verwalteten Umgebung verwenden, finden Sie auf der *Website der PGP Corporation* (http://www.pgp.com) Informationen zum Erweitern der Lizenz um PGP Whole Disk Encryption.

Ablauf der Lizenz

Wenn PGP Whole Disk Encryption unter einer Mietlizenz verwendet wird, steht nach Ablauf der Lizenz noch 90 Tage ausschließlich für Startlaufwerke eine Entschlüsselungsfunktion zur Verfügung. 90 Tage nach Ablauf der Mietlizenz werden Ihre Daten von PGP Whole Disk Encryption entschlüsselt (nach einer entsprechenden Benachrichtigung), damit Sie auf Ihre Dateien zugreifen können.

Laufwerk auf die Verschlüsselung vorbereiten

Vor der Verschlüsselung des Laufwerks müssen Sie einige Schritte ausführen, damit die erste Verschlüsselung des Laufwerks erfolgreich abläuft.

- **Vergewissern Sie sich, dass das Ziellaufwerk unterstützt wird.** Weitere Informationen finden Sie unter *Unterstützte Laufwerkstypen* (auf Seite 160).
- **Stellen Sie sicher, dass der Tastaturtyp unterstützt wird.** Weitere Informationen finden Sie unter *Unterstützte Tastaturen* (auf Seite 161).
- **Stellen Sie vor dem Verschlüsseln sicher, dass sich das Laufwerk in einwandfreiem Zustand befindet.** Falls PGP Whole Disk Encryption während der Verschlüsselung Laufwerksfehler erkennt, wird die Verschlüsselung angehalten, damit die Probleme behoben werden können. Es ist jedoch effizienter, Fehler vor dem Beginn der Verschlüsselung zu beheben. Weitere Informationen finden Sie unter *Laufwerksintegrität vor der Verschlüsselung sicherstellen* (auf Seite 164).
- **Sichern Sie das Laufwerk, bevor Sie es verschlüsseln.** Sichern Sie das Laufwerk vor der Verschlüsselung, damit keine Daten verloren gehen, wenn der Laptop oder Computer verloren geht, gestohlen wird oder Sie das Laufwerk nicht entschlüsseln können. Zudem sollten Sie regelmäßig Sicherungskopien des Laufwerks anlegen.
- **Erstellen Sie einen Wiederherstellungsdatenträger.** Obwohl die Wahrscheinlichkeit äußerst gering ist, dass ein Hauptstartdatensatz auf einem mit PGP Whole Disk Encryption verschlüsselten Startlaufwerk bzw. einer Partition beschädigt wird, kann dies nicht ausgeschlossen werden. Erstellen Sie einen Wiederherstellungsdatenträger, bevor Sie ein Startlaufwerk oder eine Partition mit PGP Whole Disk Encryption verschlüsseln. Weitere Informationen finden Sie unter *Wiederherstellungsdatenträger erstellen* (siehe "Wiederherstellungsdatenträger erstellen und verwenden" auf Seite 210).
- **Berücksichtigen Sie, wie lange die Verschlüsselung des Laufwerks dauern wird**, und bereiten Sie sich entsprechend vor. Weitere Informationen finden Sie unter *Verschlüsselungsdauer berechnen* (auf Seite 164).

- **Stellen Sie sicher, dass für die Dauer der Verschlüsselung Netzstrom zur Verfügung steht.** Weitere Informationen finden Sie unter *Netzbetrieb während der Verschlüsselung beibehalten* (auf Seite 165).
- **Führen Sie einen Pilotversuch durch, um die Softwarekompatibilität sicherzustellen.** Die PGP Corporation empfiehlt, PGP Whole Disk Encryption zur Sicherheit auf einer kleinen Gruppe von Computern zu testen, um sicherzustellen, dass kein Konflikt zwischen PGP Whole Disk Encryption und anderer auf dem Computer installierter Software besteht. Erst dann sollte die Funktion auf einer großen Anzahl von Computern bereitgestellt werden. Dies bietet sich besonders in Umgebungen an, in denen ein standardisiertes COE-Image (Corporate Operating Environment) verwendet wird. Es gibt bestimmte andere Software für den Laufwerksschutz, die nicht mit PGP Whole Disk Encryption kompatibel ist und schwerwiegende Laufwerksprobleme verursachen kann, einschließlich Datenverlust. Informationen zu bekannten Interoperabilitätsproblemen finden Sie unter *Pilotversuch zum Sicherstellen der Softwarekompatibilität durchführen* (auf Seite 166). Aktuelle Informationen zu kompatibler Software finden Sie in den *Versionshinweisen zu PGP Desktop*.
- **Stellen Sie sicher, dass Sie über die richtigen Token und Treiber verfügen.** Wenn Sie ein USB-Token zur Authentifizierung für eine mit PGP Whole Disk Encryption verschlüsselte Festplatte verwenden, achten Sie darauf, dass Sie über das richtige Token verfügen und die richtige Treiber-Software installiert ist. Weitere Informationen finden Sie unter *Token zur Verwendung für die Authentifizierung vorbereiten* (siehe "Smartcard oder Token zur Verwendung für die Authentifizierung vorbereiten" auf Seite 172).

Hinweis: Verwenden Sie PGP Whole Disk Encryption nicht zur Verschlüsselung von Serverhardware. PGP Whole Disk Encryption wird unter Windows 2000 Server oder Windows 2003 Server nicht unterstützt.

Unterstützte Laufwerkstypen

Mit PGP Whole Disk Encryption kann der Inhalt folgender Arten von Laufwerken geschützt werden:

- Desktop- oder Laptop-Laufwerke, einschließlich Solid-State-Laufwerke (entweder Partitionen oder das gesamte Laufwerk)

  Hinweis: Verwenden Sie PGP Whole Disk Encryption nicht zur Verschlüsselung von Serverhardware. PGP Whole Disk Encryption wird unter Windows 2000 Server oder Windows 2003 Server nicht unterstützt.

- Externe Laufwerke, mit Ausnahme von Musikgeräten und Digitalkameras
- USB-Flash-Laufwerke

Sie können Laufwerke oder Partitionen verschlüsseln, die mit dem Dateisystem FAT16, FAT32 oder NTFS formatiert sind. Wenn Sie PGP Whole Disk Encryption mit einem Laufwerk oder einer Partition mit einem FAT-Dateisystem verwenden, können Sie später eine Konvertierung in NTFS durchführen.

Sie können PGP Whole Disk Encryption mit einem Dual-Boot-System verwenden, wenn der Systemstart unter einem Betriebssystem erfolgt, das von PGP Whole Disk Encryption unterstützt wird (z. B. Windows XP, Windows 2000 oder Windows Vista), und wenn PGP Whole Disk Encryption installiert ist. Der Partitionsmodus unterstützt das Dual-Boot-Verfahren mit einem anderen Betriebssystem (z. B. Linux), sofern Sie lediglich die Windows-Partition verschlüsseln. Das andere Betriebssystem muss sich auf einer anderen, nicht verschlüsselten Partition befinden.

Mit PGP Whole Disk Encryption können Laufwerke beliebiger Größe verschlüsselt werden. Wenn das Laufwerk oder die Partition vom Betriebssystem (oder vom Hardware-BIOS des Startlaufwerks oder der Partition) unterstützt wird, sollte das Laufwerk oder die Partition mit PGP Desktop kompatibel sein.

Wenn Sie eine Neupartitionierung eines mit PGP Whole Disk Encryption verschlüsselten Laufwerks ausführen möchten, müssen Sie das Laufwerk zunächst entschlüsseln. Nachdem das Laufwerk entschlüsselt wurde, können Sie die Partitionierung vornehmen und die Partition(en) anschließend erneut verschlüsseln.

Alle Windows-Energieverwaltungsmodi (Ruhezustand, Standby, Bereitschaftsmodus) werden unterstützt.

Nicht unterstützte Laufwerkstypen

Folgende Laufwerkstypen werden *nicht* unterstützt:

- Dynamische Datenträger
- Disketten und CD-RW/DVD-RWs

Warnung: Unter Windows XP können Basisdatenträger in dynamische Datenträger konvertiert werden, die im Vergleich zu Basisdatenträgern verschiedene Zusatzfunktionen unterstützen. Führen Sie diese Konvertierung auf keinen Fall auf einem Startlaufwerk durch, das bereits mit PGP Whole Disk Encryption geschützt wurde. Durch die Konvertierung eines Basisdatenträgers in einen dynamischen Datenträger wird der Datenträger unbrauchbar.

Von PGP Whole Disk Encryption verwendeter Verschlüsselungsalgorithmus

PGP Whole Disk Encryption verwendet den Verschlüsselungsalgorithmus AES-256 und den Hash-Algorithmus SHA-1. Diese Optionen können nicht geändert werden.

Unterstützte Tastaturen

Stellen Sie sicher, dass Sie eine Tastatur mit einer der unterstützten Sprachen verwenden.

Im PGP Whole Disk Encryption-Anmeldebildschirm werden folgende Tastaturlayouts unterstützt:

- Belgisch (Belgien; Komma)
- Belgisch (Belgien; Punkt)
- Bosnisch (Bosnien)
- Bosnisch (Bosnien; Kyrillisch)
- Bulgarisch (Bulgarien)
- Bulgarisch (Bulgarien; Lateinisch)
- Bulgarisch (Bulgarien; Schreibmaschine)
- Kanadisch (Standard, Multilingual; Kanada)
- Chinesisch (vereinfacht; China, Singapur)
- Chinesisch (traditionell; Hongkong, Taiwan)
- Kroatisch (Kroatien)
- Tschechisch (Tschechien; QWERTY)
- Dänisch (Dänemark)
- Niederländisch (Niederlande)
- Englisch (USA)
- Englisch (Großbritannien)
- Englisch (USA, International)
- Estnisch (Estland)
- Finnisch (Finnland)
- Französisch (Belgien)
- Französisch (Kanada)
- Französisch (Frankreich)
- Französisch (Schweiz)
- Deutsch (Deutschland/Österreich)
- Deutsch (IBM)
- Deutsch (Schweiz)
- Hebräisch (Israel)
- Ungarisch (Ungarn)
- Ungarisch (Ungarn; 101 Tasten)
- Isländisch (Island)
- Irisch (Irland)
- Italienisch (Italien)

- Italienisch (Italien; 142 Tasten)
- Japanisch (Japan)
- Koreanisch (Korea)
- Norwegisch (Norwegen)
- Polnisch (Polen; Programmierer)
- Polnisch (Polen; 214-Tastatur)
- Portugiesisch (Brasilien; ABNT-Tastaturen)
- Portugiesisch (Brasilien; ABNT2-Tastaturen)
- Portugiesisch (Portugal)
- Rumänisch (Rumänien)
- Russisch (Russland; Kyrillisch)
- Serbisch (Serbien und Montenegro; Kyrillisch)
- Serbisch (Serbien und Montenegro; Lateinisch)
- Slowakisch (Slowakei)
- Slowenisch (Slowenien)
- Spanisch (Spanien)
- Spanisch (Lateinamerika)
- Spanisch (Variation)
- Schwedisch (Schweden)
- Türkisch (Türkei; F)
- Türkisch (Türkei; Q)
- Ukrainisch (Ukraine)

Bei den verschiedenen Tastaturlayouts können Zeichen unterschiedlichen Tasten zugeordnet sein. Dies kann bei der Eingabe der Passphrase zu Problemen führen. Wählen Sie das Tastaturlayout aus, das Ihrer Tastatur am besten entspricht, und verwenden Sie dieses Tastaturlayout unbedingt für jede Authentifizierung.

Weitere Informationen zu unterstützten Zeichen für Passphrasen finden Sie unter *Unterstützte Zeichen für Passphrasen für PGP Whole Disk Encryption* (siehe "Unterstütze Zeichen für Passphrasen für PGP Whole Disk Encryption" auf Seite 178).

Laufwerksintegrität vor der Verschlüsselung sicherstellen

Die PGP Corporation nimmt bei der Laufwerksverschlüsselung bewusst eine konservative Haltung ein, um Datenverlust zu verhindern. Bei der Verschlüsselung von Festplatten treten nicht selten Fehler bei der zyklischen Redundanzprüfung auf. Wenn PGP Whole Disk Encryption eine Festplatte oder Partition mit fehlerhaften Sektoren erkennt, wird der Verschlüsselungsvorgang standardmäßig unterbrochen. Während dieser Zeit können Sie das Problem beheben, bevor Sie den Verschlüsselungsvorgang fortsetzen. Auf diese Weise werden mögliche Laufwerksbeschädigungen und Datenverluste verhindert.

Damit es während der Verschlüsselung nicht zu einer Unterbrechung kommt, empfiehlt die PGP Corporation, vor der Verschlüsselung alle Laufwerksfehler zu korrigieren.

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, werden die bei der Verschlüsselung erkannten fehlerhaften Sektoren im PGP Universal Server aufgezeichnet und der Verschlüsselungsvorgang wird fortgesetzt.

Empfehlungen für bewährte Methoden

Bevor Sie versuchen, PGP Whole Disk Encryption einzusetzen, sollten Sie ein Laufwerk-Scanprogramm eines Drittanbieters verwenden, um eine Integritätsprüfung auf niedriger Stufe durchzuführen und alle Unregelmäßigkeiten des Laufwerks zu reparieren, die zu Fehlern bei der zyklischen Redundanzprüfung führen könnten. Das Programm zur Datenträgerüberprüfung von Microsoft Windows (`chkdsk.exe`) reicht nicht aus, um diese Probleme auf dem Ziellaufwerk zu erkennen. Verwenden Sie stattdessen Software wie SpinRite oder Norton Disk Doctor™. Diese Softwareanwendungen können Fehler korrigieren, die ansonsten die Verschlüsselung unterbrechen würden.

Achtung: Stark fragmentierte Laufwerke sollten vor ihrer Verschlüsselung defragmentiert werden.

Informationen zu bewährten Methoden bei der Installation von PGP Whole Disk Encryption auf einem Windows Server-System finden Sie im *PGP-Wissensdatenbankartikel 1737* (http://support.pgp.com/?faq=1737).

Verschlüsselungsdauer berechnen

Die Verschlüsselung ist zeitaufwändig und CPU-intensiv. Je größer das zu verschlüsselnde Laufwerk bzw. die zu verschlüsselnde Partition ist, desto länger dauert der Verschlüsselungsvorgang. Beachten Sie dies, wenn Sie die erstmalige Verschlüsselung des Laufwerks planen.

Die folgenden Faktoren können sich auf die Verschlüsselungsgeschwindigkeit auswirken:

- Größe des Laufwerks oder der Partition
- Prozessorgeschwindigkeit und Anzahl der Prozessoren
- Anzahl der auf dem Computer ausgeführten Systemprozesse
- Anzahl der auf dem Computer ausgeführten anderen Anwendungen
- Prozessorzeit für diese anderen Anwendungen

Auf einem durchschnittlichen System dauert die Verschlüsselung eines Startlaufwerks bzw. einer Startpartition mit einer Größe von 80 GB mit PGP Whole Disk Encryption ca. drei Stunden (wenn keine anderen Anwendungen ausgeführt werden). Auf einem sehr schnellen System kann diese Verschlüsselung hingegen in weniger als einer Stunde durchgeführt werden.

Sie können das System während der Verschlüsselung weiterhin verwenden. Das System arbeitet zwar während des Verschlüsselungsvorgangs etwas langsamer als gewöhnlich, kann jedoch uneingeschränkt verwendet werden.

PGP Desktop verlangsamt die Verschlüsselung automatisch, wenn Sie das System verwenden. Wenn Sie das System während der ersten Verschlüsselung nicht verwenden, wird der Verschlüsselungsvorgang schneller durchgeführt. Nach der Verschlüsselung arbeitet das System wieder mit normaler Geschwindigkeit.

Wenn Sie während des Verschlüsselungsvorgangs andere Anwendungen nutzen, werden diese wahrscheinlich etwas langsamer als gewohnt ausgeführt, bis die Verschlüsselung abgeschlossen ist.

Wenn Sie den Computer während der Verschlüsselung nicht verwenden, können Sie die erste Verschlüsselung mit der Option **Maximale CPU-Auslastung** beschleunigen. Weitere Informationen hierzu finden Sie unter *Verschlüsselungsoptionen festlegen* (auf Seite 170). Der Geschwindigkeitszuwachs wird dadurch erzielt, dass die Verschlüsselung Priorität gegenüber anderen Prozessen erhält, die vom Computer ausgeführt werden.

Netzbetrieb während der Verschlüsselung beibehalten

Da die Verschlüsselung CPU-intensiv ist, kann die Verschlüsselung nicht auf einem Laptop gestartet werden, der sich im Akkubetrieb befindet. Der Computer *muss* an den Netzstrom angeschlossen sein. Wenn ein Laptop während der erstmaligen Verschlüsselung (oder einer späteren Entschlüsselung bzw. Umschlüsselung) in den Akkubetrieb wechselt, wird PGP Whole Disk Encryption angehalten. Die Verschlüsselung, Entschlüsselung oder Umschlüsselung wird automatisch fortgesetzt, sobald der Computer wieder an den Netzstrom angeschlossen wird.

Unabhängig vom verwendeten Computertyp darf die Stromversorgung während der Verschlüsselung nicht unterbrochen werden oder das System anderweitig unerwartet heruntergefahren werden, sofern Sie nicht die Option **Stromausfallschutz ausgewählt haben. Ziehen Sie das Netzkabel auf keinen Fall ab, bevor der Verschlüsselungsvorgang abgeschlossen ist. Wenn es während der Verschlüsselung zu einem Stromausfall kommen kann oder wenn keine unterbrechungsfreie Stromversorgung für den Computer vorhanden ist, sollten Sie die Option Stromausfallschutz** auswählen, die unter *Verschlüsselungsoptionen einstellen* (siehe "Verschlüsselungsoptionen festlegen" auf Seite 170) beschrieben ist.

Achtung: Dies gilt ebenfalls für Wechseldatenträger, z. B. USB-Geräte. Wenn Sie nicht die Option **Stromausfallschutz** auswählen, kann das Gerät beschädigt werden, wenn Sie es während der Verschlüsselung entfernen.

Pilotversuch zum Sicherstellen der Softwarekompatibilität durchführen

Die PGP Corporation empfiehlt, PGP Whole Disk Encryption zur Sicherheit auf einer kleinen Gruppe von Computern zu testen, um sicherzustellen, dass kein Konflikt zwischen PGP Whole Disk Encryption und anderer auf dem Computer installierter Software besteht. Erst dann sollte die Funktion auf einer großen Anzahl von Computern bereitgestellt werden. Dies bietet sich besonders in Umgebungen an, in denen ein standardisiertes COE-Image (Corporate Operating Environment) verwendet wird.

Es gibt bestimmte andere Software für den Laufwerksschutz, die nicht mit PGP Whole Disk Encryption kompatibel ist und schwerwiegende Laufwerksprobleme verursachen kann, einschließlich Datenverlust. Beachten Sie die folgenden bekannten Interoperabilitätsprobleme und sehen Sie sich die aktuellen Informationen zu kompatibler Software in den Versionshinweisen zu PGP Desktop an.

Nicht kompatible Software:

- Faronics Deep Freeze (alle Versionen)
- Utimaco SafeGuard Easy 3.x
- Computrace von Absolute Software, ein Laptopsicherheits- und Tracking-Produkt. PGP Whole Disk Encryption ist nur mit der BIOS-Konfiguration von Computrace kompatibel. Die Verwendung von Computrace im MBR-Modus wird nicht unterstützt.
- Produkte zur Festplattenverschlüsselung von GuardianEdge Technologies: Dies betrifft die früher unter der Bezeichnung PC Guardian vertriebenen Produkte Encryption Anywhere Hard Disk und Encryption Plus Hard Disk.

Folgende Anwendungen können zwar mit PGP Desktop auf demselben System installiert werden, blockieren jedoch PGP Whole Disk Encryption:

- Safeboot Solo
- SecureStar SCPP

Authentifizierungsmethode für das Laufwerk bestimmen

Wenn Sie ein Laufwerk oder eine Partition mit PGP Whole Disk Encryption verschlüsseln, legen Sie fest, wie Sie sich selbst zum Entschlüsseln des Laufwerks oder der Partition authentifizieren.

Sie haben folgende Möglichkeiten:

- *Passphrasen- und Einzelanmeldungsauthentifizierung* (auf Seite 167)
- *Authentifizierung mit öffentlichen Schlüsseln* (auf Seite 168)
- *Token-basierte Authentifizierung* (auf Seite 168)
- *Zweistufige Authentifizierung mit einem USB-Flash-Gerät* (auf Seite 168)
- *Authentifizierung über das Trusted Platform Module (TPL)* (auf Seite 169)

Hinweis: Erstellen Sie auf einem Mehrbenutzersystem separate Authentifizierungsmethoden für jeden Benutzer.

Hinweis: Sie müssen Passphrasenbenutzer verwenden, wenn Benutzer mit Windows PE oder BartPE authentifiziert werden sollen. Token- oder TPM-Benutzer werden nicht unterstützt.

Passphrasen- und Einzelanmeldungsauthentifizierung

Bei der Authentifizierung mit einer Passphrase legen Sie eine Passphrase fest, die Sie beim Neustart eines mit PGP Whole Disk Encryption verschlüsselten Startlaufwerks bzw. einer Startpartition oder beim Zugriff auf ein anderes mit PGP Whole Disk Encryption verschlüsseltes Laufwerk bzw. eine Partition verwenden. Für dieses Verfahren sind weder weitere Dateien noch zusätzliche Hardware erforderlich. Es kann sowohl für Festplatten als auch für Wechseldatenträger eingesetzt werden.

Es gibt zwei Optionen für die Authentifizierung mit einer Passphrase:

- Sie können eine Passphrase auswählen, die Sie ausschließlich für PGP Whole Disk Encryption verwenden.
- Sie können die Passphrase für PGP Whole Disk Encryption mit der Windows-Kontoanmeldung synchronisieren, sodass Sie die Passphrase nur ein Mal eingeben müssen, um das verschlüsselte Laufwerk bzw. die verschlüsselte Partition zu entsperren und sich bei Windows anzumelden. Diese Synchronisierung mit der Windows-Anmeldung wird als *Einzelanmeldung* (Single Sign-On, SSO) bezeichnet.

Eine Anleitung zur Einrichtung der Einzelanmeldung finden Sie unter *Einzelanmeldung mit PGP Whole Disk Encryption verwenden* (auf Seite 190).

Authentifizierung mit öffentlichen Schlüsseln

Bei der Authentifizierung mit öffentlichen Schlüsseln legen Sie beim Verschlüsseln eines Laufwerks oder einer Partition mit PGP Whole Disk Encryption einen öffentlichen Schlüssel fest. Nur der Inhaber des entsprechenden privaten Schlüssels kann auf den Inhalt des Laufwerks oder der Partition zugreifen. Zu diesem Zweck muss der Benutzer die Passphrase seines privaten Schlüssels eingeben.

Die Authentifizierung mit öffentlichen Schlüsseln ist nur für Wechseldatenträger verfügbar, die mit dem System verwendet werden. Für Festplatten (einschließlich Startlaufwerken, Partitionen oder externen USB-Festplatten) kann entweder die Authentifizierung mit einer Passphrase oder mit einem Token genutzt werden, jedoch nicht die Authentifizierung mit öffentlichen Schlüsseln.

Token-basierte Authentifizierung

Wenn Sie eine Festplatte (einschließlich Startlaufwerk oder Startpartition) mit PGP Whole Disk Encryption verschlüsseln und zur Authentifizierung einen PGP-Schlüssel auf einem Token verwenden möchten, müssen Sie ein PGP-Schlüsselpaar auf einem Token oder einer Smartcard verwenden, das bzw. die mit PGP Whole Disk Encryption kompatibel ist. Eine Liste kompatibler Geräte finden Sie unter *Smartcards zur Authentifizierung im PGP BootGuard-Bildschirm verwenden* (siehe "Smartcards oder Token zur Authentifizierung auf dem PGP BootGuard-Bildschirm verwenden" auf Seite 173).

Die Verwendung eines Schlüsselpaars auf einem Token sorgt für zusätzliche Sicherheit, da Sie das Token mitnehmen können.

Beachten Sie, dass Sie die entsprechenden Treiber für das Gerät installieren müssen, bevor Sie mit der Laufwerksverschlüsselung beginnen können. Weitere Informationen finden Sie unter *Token zur Verwendung für die Authentifizierung vorbereiten* (siehe "Smartcard oder Token zur Verwendung für die Authentifizierung vorbereiten" auf Seite 172).

Zweistufige Authentifizierung mit einem USB-Flash-Gerät

Sie können eine zweistufige Authentifizierung verwenden, um die Datensicherheit auf dem System zu erhöhen. Die zweistufige Authentifizierung setzt sich aus etwas zusammen, das Ihnen bekannt ist (Ihre Passphrase) und etwas, über das Sie verfügen (Ihr USB-Flash-Gerät), um zu bestätigen, dass Sie die zum Zugriff auf das Laufwerk berechtigte Person sind.

Erstellen Sie bei der zweistufigen Authentifizierung einen Passphrasenbenutzer und wählen Sie dann eine weitere Form von Hardware zur Identifizierung des Benutzers aus. Sie haben die Wahl zwischen der Verwendung eines USB-Flash-Laufwerks und, sofern diese Hardware auf dem System verfügbar ist, Trusted Platform Module (TPM).

Hinweis: Wenn Sie ein USB-Flash-Gerät für die zweistufige Authentifizierung nutzen, müssen Sie den Computer bei angeschlossenem USB-Gerät neu starten, damit diese Authentifizierungsmethode wirksam wird. Bis zum Neustart mit dem USB-Gerät können Sie die Authentifizierung im PGP BootGuard-Bildschirm nur mit der Passphrase durchführen.

Weitere Informationen zum Erstellen einer zweistufigen Authentifizierung mit einem USB-Flash-Gerät finden Sie unter *Laufwerk verschlüsseln* (auf Seite 179).

Authentifizierung über das Trusted Platform Module (TPL)

Wenn das System über TPM-Hardware (Trusted Platform Module) verfügt, wird die Option zum Verwenden von TPM angezeigt. Wenn Sie einen TPM-Benutzer hinzufügen, kann sich der Benutzer nur für das Laufwerk auf diesem bestimmten System authentifizieren (der Benutzer ist spezifisch mit dem System verbunden). TPM kann nur mit Passphrasenbenutzern verwendet werden und funktioniert bei der Einzelanmeldung.

PGP Whole Disk Encryption ist mit TPM Version 1.1 oder 1.2 kompatibel.

Im Folgenden sind einige Computer aufgeführt, die TPM unterstützen und mit PGP Whole Disk Encryption kompatibel sind:

- Hewlett-Packard Compaq nx6325 (Infineon-TPM mit HP-BIOS)
- Dell D630 (Broadcom-TPM)
- Lenovo ThinkPad T60 (Atmel-TPM)
- Fujitsu LifeBook T2010, (Infineon-TPM mit Phoenix-BIOS)
- Panasonic Toughbook T5, W5 oder Y5 (Infineon-TPM mit Matsushita-BIOS)

Ihr TPM-Anbieter implementiert ggf. Sicherheitsfunktionen, die sich auf die Verwendung des TPM auswirken. Weitere Informationen finden Sie in der Dokumentation für das System.

Hinweis: Wenn Sie das TPM löschen, indem Sie es in den Auslieferungszustand zurücksetzen, oder wenn die Systemplatine mit dem TPM ersetzt wird, können Sie nicht mit dem TPM-Benutzer auf das verschlüsselte Laufwerk zugreifen, da die im TPM gespeicherten Anmeldeinformationen nicht mehr verfügbar sind. Stellen Sie sicher, dass Sie über eine andere Methode für den Zugriff auf das verschlüsselte Laufwerk verfügen (weitere Informationen finden Sie im folgenden Abschnitt „Bei der Verwendung von TPM zu beachtende Aspekte“).

Weitere Informationen zum Erstellen einer zweistufigen Authentifizierung mit dem TPM finden Sie unter *Laufwerk verschlüsseln* (auf Seite 179).

Gründe für die Verwendung von TPM

Computer mit TPM verfügen über einen integrierten Zufallszahlengenerator, der abgefragt und als Quelle für Zufallsbit verwendet werden kann. RSA-Schlüssel mit 2048 Bit können erstellt, geladen und verwendet werden. Zudem stehen Anti-Brute-Force-Funktionen zur Verfügung. Wenn eine falsche Passphrase zu oft eingegeben wird, wird das TPM gesperrt oder verlangsamt seine Reaktionen drastisch, wodurch das Erraten von Passphrasen durch die Brute-Force-Methode zu langsam und daher nutzlos wird. Auf diese Weise erhalten TPM-Schlüssel, die mit Passphrasen geschützt sind, eine viel höhere Sicherheitsstufe als es mit Software möglich ist.

Bei der Verwendung von TPM zu beachtende Aspekte

- Stellen Sie vor der Verschlüsselung des Laufwerks sicher, dass Sie die Eigentumsrechte für das TPM auf dem System festlegen, das TPM konfigurieren und dann das System neu starten, bevor Sie mit dem Verschlüsselungsvorgang beginnen. Wenn Sie die Eigentumsrechte übernehmen, richten Sie eine Passphrase für das TPM ein, die nicht für PGP Desktop oder Windows gültig ist und zum Bearbeiten des TPM verwendet wird. Durch die Übernahme der Eigentumsrechte können Sie das TPM konfigurieren und Produkte damit verwenden.
- Stellen Sie sicher, dass Sie über eine andere Methode zur Authentifizierung für das verschlüsselte Laufwerk verfügen. Wenn Sie PGP Whole Disk Encryption in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, können Sie das Whole Disk-Wiederherstellungs-Token verwenden (weitere Informationen finden Sie unter *Wiederherstellungs-Token erstellen* (auf Seite 208)). Wenn Sie PGP Whole Disk Encryption als eigenständige Anwendung verwenden, erstellen Sie zur Sicherheit einen Passphrasenbenutzer oder erstellen Sie einen Passphrasenbenutzer mit einem USB-Flash-Gerät für die zweistufige Authentifizierung (weitere Informationen finden Sie unter *Laufwerk verschlüsseln* (auf Seite 179)).

Verschlüsselungsoptionen festlegen

Nachdem Sie das Laufwerk auf die Verschlüsselung vorbereitet haben, sollten Sie die Vorgehensweise für die erstmalige Verschlüsselung erneut durchgehen:

1. Legen Sie fest, ob das gesamte Laufwerk oder nur bestimmte Partitionen verschlüsselt werden sollen. Weitere Informationen finden Sie unter *Verschlüsselung auf Partitionsebene* (auf Seite 171).
2. Legen Sie die Optionen fest, die während der Verschlüsselung angewendet werden sollen, z. B. den Stromausfallschutz oder die Verschlüsselungsgeschwindigkeit. Weitere Informationen finden Sie unter *Optionen von PGP Whole Disk Encryption verwenden* (auf Seite 175).

3 Wählen Sie die gewünschte Authentifizierungsmethode aus. Weitere Informationen finden Sie unter *Authentifizierungsmethode für das Laufwerk bestimmen* (auf Seite 167).

Hinweis: Wenn Sie die Token-basierte Authentifizierung verwenden, bereiten Sie das Token vor. Weitere Informationen finden Sie unter *Token zur Verwendung für die Authentifizierung vorbereiten* (siehe "Smartcard oder Token zur Verwendung für die Authentifizierung vorbereiten" auf Seite 172).

4 Gehen Sie bei der Verschlüsselung wie unter *Laufwerke oder Partitionen verschlüsseln* (auf Seite 177) beschrieben vor.

Hinweis: Wenn Sie ein Benutzer in einer von einem PGP Universal Server verwalteten Umgebung sind, erstellt PGP Whole Disk Encryption ein Wiederherstellungs-Token. Mit diesem Token können Laufwerke wiederhergestellt werden, für die keine Passphrasen mehr verfügbar sind. Weitere Informationen finden Sie unter *Wiederherstellungs-Token erstellen* (auf Seite 208).

Verschlüsselung auf Partitionsebene

Wenn das Laufwerk in Partitionen unterteilt ist, können Sie anstelle des gesamten Laufwerks auch einzelne Partitionen verschlüsseln. Die folgenden Verschlüsselungsmöglichkeiten sind verfügbar:

- Eine Laufwerkspartition
- Alle Laufwerkspartitionen mit Ausnahme einer einzigen Partition

Eine beliebige Anzahl von Partitionen Nur die Dateien auf den ausgewählten Partitionen werden verschlüsselt. Der Partitionsmodus unterstützt das Dual-Boot-Verfahren mit einem anderen Betriebssystem (z. B. Linux), sofern Sie lediglich die Windows-Partition verschlüsseln. Das andere Betriebssystem muss sich auf einer anderen, nicht verschlüsselten Partition befinden.

Hinweis: Nachdem ein Laufwerk oder Partitionen des Laufwerks verschlüsselt wurden, kann die Partitionierung des Laufwerks nicht mehr geändert werden (z. B. durch Hinzufügen, Entfernen oder Vergrößern bzw. Verkleinern einer Partition). Stellen Sie sicher, dass die Partitionierung des Laufwerks entsprechend Ihrer Wünsche erfolgt ist, *bevor* Sie es mit PGP Whole Disk Encryption schützen.

Smartcard oder Token zur Verwendung für die Authentifizierung vorbereiten

Wenn Sie sich für die Authentifizierung mit einer Smartcard oder einem Token entscheiden, müssen Sie ein kompatibles Gerät verwenden (eine Liste kompatibler Geräte finden Sie unter *Smartcards zur Authentifizierung auf dem PGP BootGuard-Bildschirm verwenden* (siehe "Smartcards oder Token zur Authentifizierung auf dem PGP BootGuard-Bildschirm verwenden" auf Seite 173)).

- Verwenden Sie das richtige Token-Modell.
- Fügen Sie dem verschlüsselten Laufwerk eventuell weitere Benutzer hinzu (z. B. einen Passphrasenbenutzer), damit auch bei einem Verlust des Tokens weiterhin auf das Laufwerk zugegriffen werden kann.
- Installieren Sie die Treiber des Tokens auf dem System, auf dem das Token verwendet werden soll, *bevor* Sie das Token verwenden.

Voraussetzungen für die Verwendung von Smartcards oder Token zur Authentifizierung

Überprüfen Sie vor der Verschlüsselung, ob die folgenden Voraussetzungen erfüllt sind.

Warnung: Die Sicherheit wird erhöht, wenn Sie ein Schlüsselpaar auf einem Token zur Authentifizierung für den Zugriff auf ein mit PGP Whole Disk Encryption verschlüsseltes Laufwerk oder eine Partition verwenden. Wenn Sie das Token jedoch verlieren, können Sie sich nicht mehr im PGP BootGuard-Anmeldebildschirm authentifizieren und sämtliche Daten auf dem Laufwerk bzw. der Partition gehen verloren. Aus diesem Grund sollten Sie einem Laufwerk bzw. einer Partition, das bzw. die mit PGP Whole Disk Encryption verschlüsselt ist, weitere Benutzer (Passphrase, Token oder beide) hinzuzufügen. Sollte das Token dann verloren gehen, können sich diese Benutzer authentifizieren und das Laufwerk bzw. die Partition für Sie freigeben.

- Sie können nur auf dem Token gespeicherte Schlüsselpaare verwenden. Sie müssen entweder ein Schlüsselpaar auf dem Aladdin eToken erstellen oder ein vorhandenes Schlüsselpaar an das Token senden, indem Sie mit der rechten Maustaste klicken und die Option **zum Hinzufügen aus dem Kontextmenü auswählen.**
- Wenn Sie ein Schlüsselpaar auf einem Token erstellen oder ein vorhandenes Schlüsselpaar an das Token senden, ändert sich die Passphrase für den privaten Schlüssel dieses Schlüsselpaars in die PIN-Nummer des Tokens. Für ein Aladdin eToken lautet die Standard-PIN 1234567890. Da diese Standard-PIN allgemein bekannt ist, sollten Sie sie umgehend mit den Aladdin-Konfigurationsprogrammen ändern, um die Sicherheit des Schlüsselpaars nicht zu gefährden.

Smartcards oder Token zur Authentifizierung auf dem PGP BootGuard-Bildschirm verwenden

In diesem Abschnitt werden die Systemanforderungen (kompatible Smartcards/Token und Lesegeräte) sowie Anleitungen zum Verwenden von Smartcards zur Authentifizierung im PGP BootGuard-Bildschirm beschrieben.

Kompatible Smartcardleser für die PGP Whole Disk Encryption-Authentifizierung

Die folgenden Smartcardleser werden für die Kommunikation mit einer Smartcard vor dem Systemstart unterstützt. Diese Leser können mit jeder kompatiblen, auswechselbaren Smartcard verwendet werden. Smartcard und Leser müssen nicht von demselben Hersteller sein.

Generische Smartcardleser

Die meisten CCID-Smartcardleser sind kompatibel. Die folgenden Leser wurden von der PGP Corporation getestet:

- OMNIKEY CardMan 3121 USB für Desktop-Systeme (076b:3021)
- OMNIKEY CardMan 6121 USB für mobile Systeme (076b:6622)
- ActivIdentity USB 2.0-Leser (09c3:0008)
- SCM Microsystem Smart Card Reader Modell SCR3311

CyberJack-Smartcardleser

- Reiner SCT CyberJack-PIN-Tastenfeld (0c4b:0100).

ASE-Smartcardleser

- Athena ASEDrive IIIe USB-Leser (0dc3:0802)

Eingebettete Smartcardleser

- Eingebetteter Dell D430-Leser
- Eingebetteter Dell D630-Leser
- Eingebetteter Dell D830-Leser

Kompatible Smartcards oder Token für die PGP Whole Disk Encryption-Authentifizierung

PGP Whole Disk Encryption ist für die Authentifizierung vor dem Systemstart mit den folgenden Smartcards kompatibel:

- ActiveIdentity ActivClientCAC-Smartcards, 2005 Modell
- Aladdin eToken PRO 64K, 2048-Bit-RSA-fähig

- Aladdin eToken PRO USB Key 32K, 2048-Bit-RSA-fähig
- Aladdin eToken PRO, nicht 2048-Bit-fähig (ältere Smartcards)
- Aladdin eToken PRO Java 72K
- Aladdin eToken NG-OTP 32K

Hinweis: Andere Aladdin eToken, z. B. Token mit Flash, sollten funktionieren, wenn sie mit den kompatiblen Token APDU-kompatibel sind. OEM-Versionen von Aladdin eToken, beispielsweise die von VeriSign ausgegebenen Versionen, sollten funktionieren, wenn sie mit den kompatiblen Token APDU-kompatibel sind.

- Athena ASEKey Crypto USB-Token für Microsoft ILM
- Athena ASECard Crypto-Smartcard für Microsoft ILM

Hinweis: Die Athena-Token sind nur für den Anmeldeinformationsspeicher kompatibel.

- Axalto Cyberflex Access 32K V2
- Charismathics CryptoIdentity Plug 'n' Crypt-Smartcard, nur Stick
- EMC RSA SecurID SID800-Token (v1 und 2)

Hinweis: Dieses Token ist nur für den Schlüsselspeicher kompatibel. SecurID ist nicht kompatibel.

- EMC RSA Smart Card 5200
- Marx CrypToken USB-Token
- Rainbow iKey 3000
- S-Trust StarCOS-Smartcard

Hinweis: S-Trust SECCOS-Smartcards sind nicht kompatibel.

- SafeNet iKey 2032 USB-Token
- T-Systems Telesec NetKey 3.0-Smartcard
- T-Systems TCOS 3.0 IEI-Smartcard

PIV-Karten (Personal Identity Verification)

- Oberthur ID-One Cosmo V5.2D-PIV-Karten, die die Clientsoftware ActivClient Version 6.1 verwenden.
- Giesecke- und Devrient Sm@rtCafe Expert 3.2-PIV-Karten, die die Clientsoftware ActivClient Version 6.1 verwenden.

Erforderliche Treiber für das Aladdin eToken

Bevor Sie das Aladdin eToken verwenden, müssen Sie auf dem System, auf dem das Token verwendet wird, die neuesten Softwaretreiber installieren. Microsoft Windows erkennt das Token zwar möglicherweise, auch wenn die Softwaretreiber nicht installiert sind, jedoch ist die Installation der entsprechenden Softwaretreiber für PGP Desktop *erforderlich*. Sie können die neuesten Softwaretreiber von der *Support-Website von Aladdin* (http://www.aladdin.com/support/default.asp) herunterladen.

Laden Sie die neueste Version der Treibersoftware **eToken PKI Client (RTE)** herunter (bei der Verfassung dieses Dokuments war dies Version 4.5) und installieren Sie sie auf dem System. Öffnen Sie nach Abschluss der Installation der eToken PKI-Client-Treibersoftware auf dem System PGP Desktop und klicken Sie auf das Bedienfeld für PGP Keys. Wenn die Treibersoftware ordnungsgemäß installiert wurde, wird im Bedienfeld von PGP Keys **Smartcard-Schlüssel** aufgeführt.

Wenn Sie **Benutzer eines Token-Schlüssels** als Authentifizierungsmethode für das mit PGP Whole Disk Encryption verschlüsselte Laufwerk bzw. die Partition angeben und im Feld **Schlüssel auswählen** der Eintrag **Kein passender Schlüssel verfügbar** angezeigt wird, kann dies auf eines der folgenden Probleme hinweisen:

- Das Aladdin eToken ist nicht eingesetzt.
- Die Treibersoftware weist die falsche Version auf oder wurde nicht ordnungsgemäß installiert.
- Das Schlüsselpaar auf dem Token kann nicht verwendet werden oder es befindet sich kein Schlüssel auf dem eToken (d. h. das eToken ist leer).

Optionen von PGP Whole Disk Encryption verwenden

In PGP Whole Disk Encryption sind zwei Optionen verfügbar, die Sie vor dem Schützen eines Laufwerks oder einer Partition auswählen können:

- **Maximale CPU-Auslastung:** Dies ist die schnellste Variante, um ein Laufwerk mit PGP Whole Disk Encryption erstmalig zu verschlüsseln, ohne Kompromisse bei der Sicherheit einzugehen. Der Geschwindigkeitszuwachs wird dadurch erzielt, dass die Verschlüsselung Priorität gegenüber anderen Prozessen erhält, die vom Computer ausgeführt werden. Wählen Sie diese Option, wenn Sie den Computer während der Verschlüsselung nicht anderweitig nutzen möchten.

- **Stromausfallschutz:** Die erstmalige Verschlüsselung kann jederzeit unterbrochen werden, indem der Computer ordnungsgemäß heruntergefahren oder neu gestartet wird. Es sollte jedoch unbedingt vermieden werden, dass der Computer unerwartet abgeschaltet wird, z. B. durch Stromausfall, versehentliches Herausziehen des Netzkabels usw. Wenn dies nicht völlig ausgeschlossen werden kann oder wenn keine unterbrechungsfreie Stromversorgung zur Verfügung steht, sollten Sie eventuell die Option **Stromausfallschutz** auswählen. Wenn die Option **Stromausfallschutz** aktiviert ist, wird die Verschlüsselung im Journal erfasst. Auf diese Weise kann der Verschlüsselungsvorgang nach einer Unterbrechung der Stromversorgung sicher und zuverlässig fortgesetzt werden. Allerdings kann die erstmalige Verschlüsselung mit dieser Option um ein Vielfaches länger dauern.

  Diese Option bietet sich auch bei der Verschlüsselung von USB-Geräten an. Sollte die Verschlüsselung unterbrochen werden, indem das USB-Gerät während der Verschlüsselung entfernt wird, kann das Gerät beschädigt werden und muss gegebenenfalls neu formatiert werden. Die Verschlüsselung im Modus für den Stromausfallschutz ermöglicht Ihnen, das USB-Gerät während der Verschlüsselung zu entfernen und mit der Verschlüsselung fortzufahren, nachdem es wieder angeschlossen wurde.

Die folgende Tabelle erleichtert die Auswahl der Optionen, die individuell am besten geeignet sind:

Ausgewählte Option	Vorteile	Anmerkungen
Keine Option (normal)	Geschwindigkeit und Sicherheit sind bei der Verschlüsselung des Laufwerks oder der Partition gleichwertig. Der Computer kann während der Verschlüsselung verwendet werden. Diese Option ist für die meisten Benutzer am besten geeignet.	Die Verschlüsselung läuft mit der Standardgeschwindigkeit ab. Es muss sichergestellt sein, dass der Computer nicht unerwartet abgeschaltet wird, da es andernfalls zu Datenverlust kommen kann.
Maximale CPU-Auslastung	Die Verschlüsselung des Laufwerks oder der Partition erfolgt schneller als im normalen Modus. Trotz der erhöhten Geschwindigkeit wird die Sicherheit der Verschlüsselung im	Diese Option erfordert maximale Computerleistung. Das System reagiert daher während der Verschlüsselung des Laufwerks oder der Partition erheblich langsamer.

Ausgewählte Option	Vorteile	Anmerkungen
	Vergleich zum normalen Modus nicht beeinträchtigt.	
Stromausfallschutz	Das Laufwerk oder die Partition wird mit einem Verfahren verschlüsselt, das auch nach einer plötzlichen Unterbrechung der Stromversorgung problemlos und sicher fortgesetzt werden kann. Diese Option eignet sich für Standorte, an denen keine unterbrechungsfreie Stromversorgung zur Verfügung steht.	Die Verschlüsselung dauert erheblich länger als im normalen Modus.
Beide Optionen	Das Laufwerk oder die Partition ist durch die Verwendung des Stromausfallschutzes besonders geschützt. Die Verschlüsselung erfolgt schneller, als wenn nur die Option „Stromausfallschutz“ ausgewählt ist.	Dennoch ist der Zeitbedarf erheblich höher als im normalen Modus.

Laufwerke oder Partitionen verschlüsseln

Wenn Sie das Laufwerk vorbereitet und die Verschlüsselungsoptionen festgelegt haben, können Sie das Laufwerk oder die Partition verschlüsseln. Beachten Sie zuvor folgende Punkte:

- Wenn Sie ein USB-Token zur Authentifizierung für eine mit PGP Whole Disk Encryption verschlüsselte Festplatte verwenden, achten Sie darauf, dass Sie über das richtige Token verfügen und die richtige Treiber-Software installiert ist. Weitere Informationen finden Sie unter *Token-basierte Authentifizierung* (auf Seite 168).

  Hinweis: Die Token-basierte Authentifizierung ist nicht für die Einzelanmeldung verfügbar.

- Das System arbeitet zwar während des Verschlüsselungsvorgangs etwas langsamer als gewöhnlich, kann jedoch uneingeschränkt verwendet werden. Nach der Verschlüsselung arbeitet es wieder mit normaler Geschwindigkeit.

  PGP Desktop verlangsamt die Verschlüsselung automatisch, wenn Sie das System verwenden. Wenn Sie das System während der ersten Verschlüsselung nicht verwenden, wird der Verschlüsselungsvorgang schneller durchgeführt.

- Sie können PGP Desktop während der Verschlüsselung minimieren oder schließen. Dies hat keine Auswirkungen auf den Prozess, erhöht jedoch die Geschwindigkeit des Verschlüsselungsvorgangs.

- Unterbrechen Sie die Verschlüsselung vorübergehend, indem Sie auf **Anhalten** und danach im Dialogfeld auf **Pause** klicken. Klicken Sie auf **Fortsetzen**, um den Vorgang wieder zu starten. Nachdem Sie auf **Fortsetzen geklickt haben, müssen Sie sich möglicherweise authentifizieren.**

- Wenn Sie das System vor Abschluss des Verschlüsselungsvorgangs herunterfahren möchten, fahren Sie es normal herunter. Sie müssen die Verschlüsselung dazu nicht anhalten. Beim nächsten Systemstart wird der Verschlüsselungsvorgang automatisch an dem Punkt fortgesetzt, an dem er unterbrochen wurde.

- Sie können jeweils immer nur ein Laufwerk bzw. eine Partition verschlüsseln, entschlüsseln bzw. umschlüsseln. Wenn Sie eine dieser Operationen für ein Laufwerk oder eine Partition starten, können Sie erst nach Abschluss der ersten Operation einen weiteren Verschlüsselungsvorgang beginnen. Dies kann auch nicht durch Anhalten der ersten Operation umgangen werden.

Unterstütze Zeichen für Passphrasen für PGP Whole Disk Encryption

PGP Whole Disk Encryption unterstützt beim Erstellen von Passphrasen alphanumerische Zeichen, Interpunktionszeichen, Standard-Metazeichen und erweiterte ASCII-Zeichen. Tabulatorzeichen und Steuerzeichen werden nicht unterstützt. Beachten Sie bei der Auswahl einer Passphrase die folgenden Punkte.

The following characters are supported: `abcdefghijklmnopqrstuvwxyz ABCDEFGHIJKLMNOPQRSTUVWXYZ`

0123456789

`~!@#$%^&*()_+={}\|:;[]'"<>,.?/-

- Most extended ASII characters (such as ç é è ê ë î ï ô û ù ü ÿ) or symbols (such as ¢ ® œ), are supported.

In der folgenden Tabelle finden Sie eine Liste der Zeichen, die bei der Eingabe als Teil einer Passphrase für die entsprechende Tastatur nicht unterstützt werden:

Tastatur	Nicht unterstützte Zeichen
Italienisch (Italien)	`~
Hebräisch (Israel)	abcdefghijklmnopqrstuvwxyz`
Russisch (Russland)	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ`@#$^&{}|[]'<>~
Bosnisch (Bosnien; Kyrillisch)	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ
Bulgarisch (Bulgarien)	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUWXYZ'[]<>{}@#$^&*
Polnisch (Polen; 214 Tasten)	[]|
Serbisch (Serbien; Kyrillisch)	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ[]{}|@^
Ukrainisch (Ukraine)	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ'[]`<>{}|~@#$^&

Laufwerk verschlüsseln

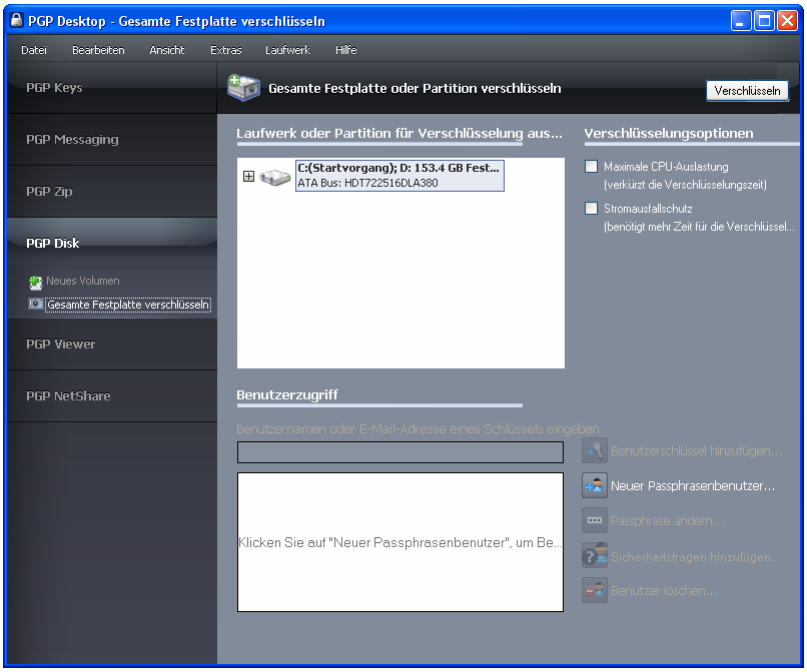
Sichern Sie das Laufwerk vor der Verschlüsselung, damit keine Daten verloren gehen, wenn der Laptop oder Computer verloren geht, gestohlen wird oder Sie das Laufwerk nicht entschlüsseln können.

Sie können jeweils immer nur ein Laufwerk bzw. eine Partition verschlüsseln, entschlüsseln bzw. umschlüsseln. Wenn Sie eine dieser Operationen für ein Laufwerk oder eine Partition starten, können Sie erst nach Abschluss der ersten Operation einen weiteren Verschlüsselungsvorgang beginnen. Dies kann auch nicht durch Anhalten der ersten Operation umgangen werden.

So schützen Sie ein Laufwerk bzw. eine Partition mit PGP Whole Disk Encryption

1 Öffnen Sie PGP Desktop und klicken Sie auf das Bedienfeld für PGP Disk. Das Bedienfeld für PGP Disk wird hervorgehoben.

2 Klicken Sie auf **Gesamte Festplatte verschlüsseln**. Der Arbeitsbereich für das Verschlüssen der gesamten Festplatte (Partition) wird angezeigt und in einer Liste sind die Laufwerke des Systems aufgeführt, die mit PGP Whole Disk Encryption geschützt werden können: Laufwerke, Laufwerkspartitionen, Wechseldatenträger usw.



3 Klicken Sie im Arbeitsbereich zum Verschlüsseln der gesamten Festplatte oder Partition oben im Bereich **Laufwerk oder Partition für Verschlüsselung auswählen**, um das Laufwerk bzw. die Partition auf dem Computer auszuwählen, das bzw. die Sie mit PGP Whole Disk Encryption verschlüsseln möchten.

4 Wählen Sie bei Bedarf die gewünschten **Verschlüsselungsoptionen aus. Weitere Informationen zu den Auswahlmöglichkeiten finden Sie unter** *Optionen von PGP Whole Disk Encryption verwenden* (auf Seite 175).

5 Legen Sie im Bereich **Benutzerzugriff** fest, wie Sie auf das geschützte Laufwerk bzw. die geschützte Partition zugreifen möchten:

- **Benutzer eines Token-basierten öffentlichen Schlüssels**: Wählen Sie diese Option, wenn Sie eine Festplatte (keinen Wechseldatenträger) auf dem System schützen möchten.

- Geben Sie den Benutzernamen oder die E-Mail-Adresse für den Schlüssel ein und drücken Sie die **Eingabetaste**, um nach dem Schlüssel zu suchen. Sie können auch **Benutzerschlüssel hinzufügen** auswählen. Eine Liste der Schlüsselpaare auf dem Schlüsselbund wird angezeigt. Wählen Sie im Feld „Schlüsselquelle“ die gewünschten öffentlichen Schlüssel aus. Klicken Sie auf **Hinzufügen**, um die Schlüssel in das Feld **Hinzuzufügende Schlüssel** zu verschieben und klicken Sie auf **OK**. Klicken Sie auf **Verschlüsseln**.

- **Passphrasenbenutzer**. Wenn Sie das Laufwerk oder die Partition mit einer Passphrase schützen möchten, wählen Sie **Neuer Passphrasenbenutzer** aus. Das Dialogfeld „PGP Disk-Assistent: Whole Disk Encryption - Neuer Benutzer“ wird angezeigt.

  - **Wählen Sie zum Entsperren des verschlüsselten Laufwerks mit der Windows-Kontoanmeldung** die Option **Windows-Kennwort verwenden** aus und klicken Sie auf **Weiter.** Wählen Sie im Dialogfeld „Zweistufige Authentifizierung“ des PGP Disk-Assistenten die Option **Nur mit Authentifizierung mit einer Passphrase fortfahren** aus und klicken Sie auf **Weiter**. Geben Sie im Dialogfeld „Windows-Kontoanmeldung“ des PGP Disk-Assistenten den Benutzernamen, die Domäne und das Kennwort für Windows ein und klicken Sie auf **Weiter**. Klicken Sie auf **Beenden**.

  Wenn Sie die Option **Windows-Kennwort verwenden** ausgewählt haben, geben Sie nach der ersten Verschlüsselung beim Systemstart im PGP BootGuard-Anmeldebildschirm das Windows-Kennwort ein. Sie werden von der PGP-Funktion für die Einzelanmeldung automatisch bei Windows angemeldet und müssen die Passphrase nur einmal eingeben. (Das ist die Einzelanmeldungsfunktion. Weitere Informationen finden Sie unter *Einzelanmeldung mit PGP Whole Disk Encryption verwenden* (auf Seite 190).)

  - **Wählen Sie zum Entsperren des verschlüsselten Laufwerks bzw. der verschlüsselten Partition mit einer neuen Passphrase** die Option **Neue Passphrase erstellen aus und klicken Sie auf Weiter**. Wählen Sie im Dialogfeld „Zweistufige Authentifizierung“ des PGP Disk-Assistenten die Option **Nur mit Authentifizierung mit einer Passphrase fortfahren** aus und klicken Sie auf **Weiter**. Geben Sie im Dialogfeld „Benutzernamen und Passphrase erstellen“ des PGP Disk-Assistenten den Namen des neuen Benutzers und die Passphrase ein, die Sie dem Benutzer zuordnen möchten. Geben Sie die Passphrase in das Feld **Bestätigen erneut ein und klicken Sie auf Weiter**. Klicken Sie auf **Beenden**.

  - **Wählen Sie zum Entsperren des verschlüsselten Laufwerks bzw. der verschlüsselten Partition mit zweistufiger Authentifizierung mit einer Passphrase und einem USB-Flash-Laufwerk** die Option **Neue Passphrase erstellen aus und klicken Sie auf Weiter**.

Wählen Sie im Dialogfeld „Zweistufige Authentifizierung“ des PGP Disk-Assistenten die Option **Generisches USB-Flash-Gerät** und dann das Gerät in der Liste aus. Klicken Sie auf **Weiter**. Geben Sie im Dialogfeld „Benutzernamen und Passphrase erstellen“ des PGP Disk-Assistenten den Namen des neuen Benutzers und die Passphrase ein, die Sie dem Benutzer zuordnen möchten. Geben Sie die Passphrase in das Feld **Bestätigen** **erneut ein und klicken Sie auf** **Weiter**. Klicken Sie auf **Beenden**.

- **Wählen Sie zum Entsperren des verschlüsselten Laufwerks bzw. der verschlüsselten Partition mit zweistufiger Authentifizierung mit einer Passphrase und TPM** die Option **Neue Passphrase erstellen** **aus und klicken Sie auf** **Weiter**. Wählen Sie im Dialogfeld „Zweistufige Authentifizierung“ des PGP Disk-Assistenten die Option **Trusted Platform Module** aus und klicken Sie auf **Weiter**. Geben Sie im Dialogfeld „Benutzernamen und Passphrase erstellen“ des PGP Disk-Assistenten den Namen des neuen Benutzers und die Passphrase ein, die Sie dem Benutzer zuordnen möchten. Geben Sie die Passphrase in das Feld **Bestätigen** **erneut ein und klicken Sie auf** **Weiter**. Klicken Sie auf **Beenden**.

Als zusätzliche Sicherheitsmaßnahme werden die für die Passphrase eingegebenen Zeichen in der Regel nicht auf dem Bildschirm angezeigt. Wenn Sie jedoch sicher sind, dass Sie nicht beobachtet werden (weder physisch über Ihre Schulter noch durch Abfangen der vom Monitor ausgestrahlten Signale) und die Zeichen beim Eingeben der Passphrase anzeigen möchten, aktivieren Sie das Kontrollkästchen **Tastatureingabe anzeigen**. Weitere Informationen finden Sie unter *Die Passphrasen-Qualitätsanzeige* (auf Seite 352).

Achtung: Sie sollten unbedingt ein unterstütztes Tastaturlayout verwenden, wenn Sie eine Passphrase für ein mit PGP Whole Disk Encryption verschlüsseltes Laufwerk bzw. eine Partition erstellen (weitere Informationen finden Sie unter *Unterstützte Tastaturen* (auf Seite 161)). Die Passphrase zur Authentifizierung muss im Anmeldebildschirm von PGP Whole Disk Encryption mit einem dieser Tastaturlayouts eingegeben werden. Ein anderes Tastaturlayout kann zu Problemen bei der Authentifizierung führen. Weitere Informationen finden Sie unter *Authentifizierung im PGP BootGuard-Bildschirm* (auf Seite 184).

6. Vergewissern Sie sich, dass der gewünschte Benutzerzugriff konfiguriert ist und klicken Sie auf **Verschlüsseln**.
7. Lesen Sie die angezeigten Informationen und klicken Sie auf **OK**.
8. Den Fortgang der Verschlüsselung des Laufwerks können Sie der Anzeige **Verschlüsselungsfortschritt** entnehmen.
9. Unterbrechen Sie die Verschlüsselung vorübergehend, indem Sie auf **Anhalten** und danach im Dialogfeld auf **Pause** klicken. Klicken Sie auf **Fortsetzen**, um den Vorgang fortzusetzen. Sie werden möglicherweise zur Eingabe der entsprechenden Passphrase aufgefordert.

Hinweis: Wenn der Verschlüsselungsvorgang unterbrochen wird und PGP Desktop einen Schreib-/Lesefehler meldet, wurden von PGP Desktop während der Verschlüsselung fehlerhafte Sektoren auf dem Laufwerk bzw. der Partition erkannt. Sie können die Verschlüsselung fortsetzen oder den Vorgang abbrechen und die Fehler beheben. Weitere Informationen finden Sie unter *Laufwerksfehler während der Verschlüsselung* (auf Seite 183). Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, werden die bei der Verschlüsselung erkannten fehlerhaften Sektoren im PGP Universal Server aufgezeichnet und der Verschlüsselungsvorgang wird fortgesetzt.

Wenn der Verschlüsselungsvorgang abgeschlossen wurde, wird im Abschnitt „Benutzerzugriff“ der Benutzer angezeigt, den Sie für die Verschlüsselung verwendet haben. Darüber hinaus werden weitere Benutzerzugriffsoptionen verfügbar, sodass Sie einen neuen Benutzer hinzufügen, die Passphrase ändern oder einen Benutzer löschen können.

10 Die PGP Corporation empfiehlt, nach der Verschlüsselung des Laufwerks einen Wiederherstellungsdatenträger zu erstellen. Weitere Informationen finden Sie unter *Wiederherstellungsdatenträger erstellen* (siehe "Wiederherstellungsdatenträger erstellen und verwenden" auf Seite 210).

Laufwerksfehler während der Verschlüsselung

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, werden die bei der Verschlüsselung erkannten fehlerhaften Sektoren im PGP Universal Server aufgezeichnet und der Verschlüsselungsvorgang wird fortgesetzt.

Viele Festplatten weisen fehlerhafte Sektoren auf. Falls PGP Whole Disk Encryption während der Verschlüsselung fehlerhafte Sektoren erkennt, wird die Verschlüsselung angehalten. Es wird eine Warnung ausgegeben, dass von PGP Whole Disk Encryption Laufwerksfehler erkannt wurden. (Beachten Sie, dass diese Fehler nicht mit der Verschlüsselung zusammenhängen. Sie weisen lediglich darauf hin, dass die Festplatte gewartet werden muss.)

Sie haben folgende Möglichkeiten:

- Erzwingen Sie die Fortsetzung der Verschlüsselung, indem Sie auf **Ja** klicken. Laufwerksfehler treten häufig auf und sind oft harmlos. Durch Klicken auf **Ja** wird der Verschlüsselungsvorgang fortgesetzt und PGP Whole Disk Encryption ignoriert weitere Fehler.
- Halten Sie die Verschlüsselung an, indem Sie auf **Nein** klicken und entschlüsseln Sie die Festplatte vollständig. Reparieren Sie anschließend die Laufwerksfehler mit einem Tool wie SpinRite oder Norton Disk Doctor, bevor Sie erneut versuchen, die Festplatte zu verschlüsseln. Wenn es Anzeichen dafür gibt, dass die Festplatte stark fragmentiert ist oder viele Sektoren fehlerhaft sind, sollten Sie unverzüglich die erforderliche Wartung durchführen, bevor Sie die Festplatte verschlüsseln.

Mit PGP Whole Disk Encryption verschlüsselte Laufwerke verwenden

Wenn Sie das Startlaufwerk (oder eine sekundäre Festplatte) des Systems mit PGP Whole Disk Encryption schützen, ändert sich das Verhalten beim Systemstart. Nach dem Einschalten wird zunächst der PGP BootGuard-Anmeldebildschirm angezeigt, in dem Sie zur Eingabe der Passphrase aufgefordert werden.

PGP Whole Disk Encryption entschlüsselt dann das Laufwerk. Wenn Sie die Einzelanmeldungsfunktion aktiviert haben (d. h. Sie haben die Passphrase von PGP Whole Disk Encryption mit der Windows-Kontoanmeldung synchronisiert), werden Sie auch bei Windows angemeldet.

Wenn Sie ein mit PGP Whole Disk Encryption verschlüsseltes Laufwerk verwenden, wird es automatisch bei Bedarf entschlüsselt und geöffnet. Nachdem ein Laufwerk vollständig verschlüsselt wurde, ist auf den meisten neueren Computern keine merkliche Geschwindigkeitseinbuße festzustellen.

Nachdem Sie ein Laufwerk oder eine Partition entsperrt haben, stehen die darauf befindlichen Dateien nicht nur Ihnen, sondern allen Personen zur Verfügung, die physischen Zugriff zu dem System haben. Die Dateien bleiben so lange entsperrt, bis Sie den Computer herunterfahren und die Dateien dadurch wieder sperren.

Warnung: Da die Dateien so lange entsperrt bleiben, bis Sie sie wieder sperren, sollten Sie die Verwendung eines PGP Virtual Disk-Laufwerks für Dateien in Betracht ziehen, die gesichert sein müssen, während der Computer verwendet wird. Weitere Informationen finden Sie unter *PGP Virtual Disk-Laufwerke verwenden* (auf Seite 219).

Wenn Sie ein System mit einem verschlüsselten Startlaufwerk bzw. einer verschlüsselten Startpartition herunterfahren oder neu starten oder einen verschlüsselten Wechseldatenträger vom System entfernen, bleiben alle Dateien auf dem Laufwerk bzw. der Partition verschlüsselt und vollständig geschützt. Daten werden niemals in einem nicht verschlüsselten Format auf das Laufwerk bzw. die Partition geschrieben. Damit wieder auf die Dateien zugegriffen werden kann, ist die korrekte Authentifizierung (Passphrase, Token oder privater Schlüssel) erforderlich.

Authentifizierung im PGP BootGuard-Bildschirm

Es gibt zwei mögliche Gründe dafür, dass Sie im PGP BootGuard-Anmeldebildschirm zur Eingabe der richtigen Passphrase für das geschützte Laufwerk bzw. die geschützte Partition aufgefordert werden:

- Wenn das Startlaufwerk bzw. die Startpartition mit PGP Whole Disk Encryption geschützt ist, müssen Sie sich ordnungsgemäß authentifizieren, damit der Systemstart erfolgen kann. Dies ist erforderlich, da die Betriebssystemdateien, die den Systemstart steuern, verschlüsselt sind und entschlüsselt werden müssen, bevor sie zum Starten des Systems verwendet werden können. Wenn Sie bei der ersten Verschlüsselung des Startlaufwerks bzw. der Startpartition die Einzelanmeldungsfunktion angegeben haben, erfolgt über die Einzelanmeldungsfunktion der PGP-Anwendung auch die Anmeldung bei Windows.
- Wenn eine sekundäre Festplatte oder Partition mit PGP Whole Disk Encryption geschützt ist, können Sie sich beim Systemstart authentifizieren. Es ist dann keine Authentifizierung mehr erforderlich, wenn Sie später auf Dateien auf der sekundären Festplatte oder Partition zugreifen möchten. Da die Dateien auf der sekundären Festplatte oder Partition (die nicht zum Starten verwendet wird) für den Systemstart nicht erforderlich sind, werden Sie beim Systemstart nicht zur Authentifizierung aufgefordert. Wenn Sie über Administratorrechte verfügen und diese Vorgehensweise von der PGP Universal Server-Richtlinie unterstützt wird, können Sie die Funktion „Umgehen“ verwenden, um die Authentifizierung beim Systemstart zu überspringen. Sie werden dann später zur Authentifizierung aufgefordert, wenn Sie Dateien auf der sekundären Festplatte oder Partition verwenden möchten.

Hinweis: Im PGP BootGuard-Anmeldebildschirm werden die Authentifizierungsdaten aller Benutzer akzeptiert, die für ein verschlüsseltes Laufwerk oder eine verschlüsselte Partition konfiguriert sind. Wenn beispielsweise auf einem System zwei Benutzer für ein Startlaufwerk bzw. eine Startpartition und zwei weitere Benutzer für eine sekundäre Festplatte bzw. Partition konfiguriert sind, kann sich *jeder* dieser vier konfigurierten Benutzer beim Systemstart mit seiner Passphrase im PGP BootGuard-Anmeldebildschirm authentifizieren. Dies umfasst auch die zwei Benutzer, die auf der sekundären Festplatte bzw. Partition konfiguriert sind.

Sie haben im PGP BootGuard-Anmeldebildschirm folgende Möglichkeiten:

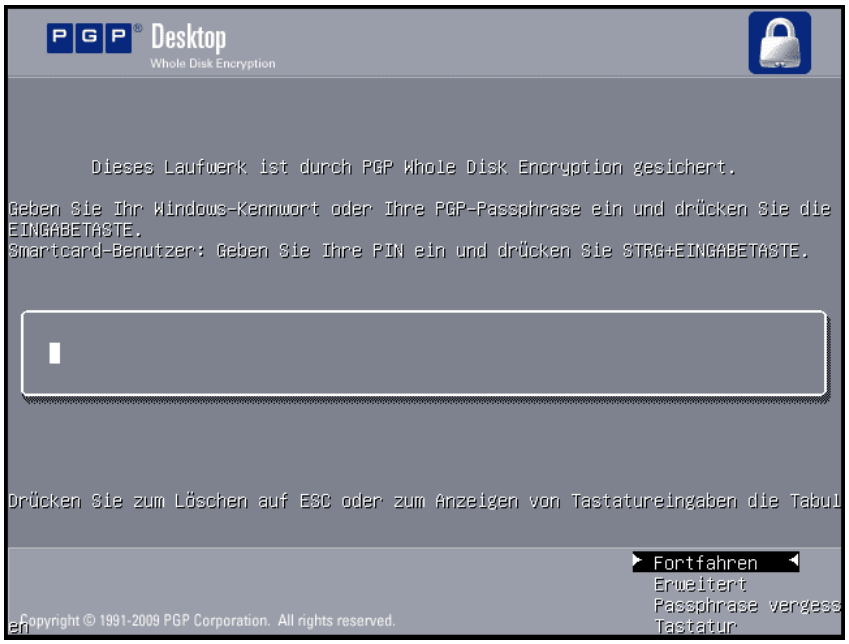
- Authentifizieren Sie sich an einem verschlüsselten Start- oder sekundärem Laufwerk bzw. an einer verschlüsselten Start- oder sekundären Partition im System.
- Zeigen Sie Informationen zu den Laufwerken und Partitionen des Systems an und greifen Sie auf die Funktion „Umgehen“ zu (die Funktion „Umgehen“ kann nur von Benutzern mit Administratorrechten verwendet werden und nur, wenn dies gemäß der PGP Universal Server-Richtlinie zulässig ist).
- Wählen Sie das Tastaturlayout aus.

Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, hat der PGP-Administrator möglicherweise den PGP Whole Disk Encryption BootGuard-Bildschirm angepasst, damit zusätzlicher Text oder ein eigenes Bild, z. B. das Logo der Organisation, angezeigt wird. Die in diesem Handbuch enthaltenen Abbildungen entsprechen der Standardinstallation. Der Ihnen angezeigte Anmeldebildschirm sieht möglicherweise anders aus, wenn er vom Administrator angepasst wurde.

So authentifizieren Sie sich im PGP BootGuard-Anmeldebildschirm

1 Führen Sie einen Start oder Neustart des Systems aus, auf dem ein Laufwerk bzw. eine Partition mit PGP Whole Disk Encryption verschlüsselt ist. Beim Systemstart wird der PGP BootGuard-Anmeldebildschirm angezeigt.

Hinweis: Wenn Sie ein USB-Gerät für die zweistufige Authentifizierung verwenden, müssen Sie sicherstellen, dass das USB-Gerät ordnungsgemäß eingelegt ist *bevor* Sie das System starten oder neu starten.


PGP Desktop
Whole Disk Encryption
Dieses Laufwerk ist durch PGP Whole Disk Encryption gesichert.
Geben Sie Ihr Windows-Kennwort oder Ihre PGP-Passphrase ein und drücken Sie die EINGABETASTE.
Smartcard-Benutzer: Geben Sie Ihre PIN ein und drücken Sie STRG+EINGABETASTE.
Drücken Sie zum Löschen auf ESC oder zum Anzeigen von Tastatureingaben die Tabul
Fortfahren
Erweitert
Passphrase vergess
Tastatur
en
Copyright © 1991-2009 PGP Corporation. All rights reserved.

2 Geben Sie eine gültige Passphrase oder ein gültiges Windows-Kennwort ein und drücken Sie die **Eingabetaste**.

Achtung: Die Passphrase muss im Anmeldebildschirm von PGP Whole Disk Encryption mit einem dieser unterstützten Tastaturlayouts eingegeben werden. Wenn Sie beim Erstellen der Passphrase für ein mit PGP Whole Disk Encryption geschütztes Laufwerk bzw. eine geschützte Partition ein anderes Tastaturlayout verwendet haben, können bei der Authentifizierung möglicherweise Probleme auftreten, da die Zuordnungen der Tasten der unterschiedlichen Tastaturlayouts eventuell nicht identisch sind. Weitere Informationen finden Sie unter *Tastaturlayouts festlegen* (auf Seite 188).

Damit die Zeichen bei der Eingabe angezeigt werden, drücken Sie vor der Eingabe die **Tabulatortaste**.

Falls Sie sich bei der Eingabe verschreiben oder möglicherweise verschrieben haben, drücken Sie die Taste **Esc**, um alle Zeichen zu löschen und die Eingabe zu wiederholen.

Wenn die lokale Selbstwiederherstellung konfiguriert wurde und Sie Ihre Passphrase vergessen haben, wählen Sie die Option **Passphrase vergessen** aus. Weitere Informationen finden Sie unter *Lokale Selbstwiederherstellung verwenden* (siehe "Vorgehensweise bei vergessenen Passphrasen" auf Seite 200).

Hinweis: Für die Token-Authentifizierung in PGP BootGuard müssen Sie zusätzlich zur Eingabetaste gleichzeitig auch die Strg-Taste drücken. Die Authentifizierung mit Token in PGP BootGuard kann eine gewisse Zeit in Anspruch nehmen.

3 Wenn Sie eine gültige Passphrase eingegeben haben, wird der PGP BootGuard-Anmeldebildschirm ausgeblendet und das System wird normal gestartet.

Wenn Sie bei der erstmaligen Verschlüsselung des Startlaufwerks die Windows-Kontoanmeldung zur Authentifizierung gewählt haben, werden Sie von PGP Whole Disk Encryption bei Windows angemeldet. Sie müssen die Passphrase nur einmal eingeben.

Wenn Sie eine ungültige Passphrase eingegeben haben, wird eine Fehlermeldung angezeigt. Geben Sie die Passphrase in diesem Fall erneut ein.

Akustische Signale während der Authentifizierung

Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen und der PGP-Administrator diese Option aktiviert hat, gibt das System während der PGP BootGuard-Authentifizierung akustische Signale aus. Es gibt drei verschiedene Tonpaare. Mit einem Tonpaar wird der Zeitpunkt für die Eingabe der Passphrase angezeigt und mit den anderen beiden jeweils der Erfolg oder das Fehlschlagen der Authentifizierung.

Jedes Signal beginnt mit einem Ton mittlerer Tonhöhe und der zweite Ton ist entweder höher, gleich oder niedriger.

- Wenn das System erstmalig zur Eingabe der Passphrase bzw. des PIN bereit ist, wird zwei Mal der Ton mittlerer Tonhöhe ausgegeben (bereit). Wenn Sie diesen Ton hören, geben Sie die Passphrase ein und drücken Sie die Eingabetaste.
- Nachdem Sie eine Passphrase eingegeben haben, ist die Tonausgabe vom Erfolg oder Fehlschlagen der Passphraseneingabe abhängig.
  - Wenn die Passphrasen-Authentifizierung erfolgreich war, wird der mittlere und dann der hohe Ton ausgegeben. Das System setzt den Systemstart daraufhin fort.
  - Wenn die Passphrasen-Authentifizierung nicht erfolgreich war, wird der mittlere und dann der niedrige Ton ausgegeben. Dann wird der PGP BootGuard-Bildschirm für die Authentifizierung angezeigt und die Eingabe aus dem Passphrasen-Feld gelöscht, damit Sie die Passphrase erneut eingeben können.

Diese akustischen Signaltöne können vom PGP-Administrator nicht individuell angepasst werden. Der Administrator kann lediglich angeben, ob akustische Signale während der PGP BootGuard-Authentifizierung aktiviert sein sollen.

Im PGP BootGuard-Bildschirm ausgesperrte Benutzer

Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, hat der PGP-Administrator u. U. eine PGP BootGuard-Aussperrung festgelegt. Sie sind „ausgesperrt“, wenn Sie die maximal zulässige Anzahl an Passphrasen-Eingabeversuchen im PGP BootGuard-Bildschirm überschritten haben. Dies gilt nur für Passphrasenbenutzer (Token- oder TPM-Benutzer sind nicht betroffen).

Wenden Sie sich an den PGP-Administrator, um die Sperre aufheben zu lassen.

Tastaturlayouts festlegen

Im PGP Whole Disk Encryption-Anmeldebildschirm werden folgende Tastaturlayouts unterstützt:

- Belgisch (Belgien; Komma)
- Belgisch (Belgien; Punkt)
- Bosnisch (Bosnien)
- Bosnisch (Bosnien; Kyrillisch)
- Bulgarisch (Bulgarien)
- Bulgarisch (Bulgarien; Lateinisch)
- Bulgarisch (Bulgarien; Schreibmaschine)
- Kanadisch (Standard, Multilingual; Kanada)
- Chinesisch (vereinfacht; China, Singapur)

- Chinesisch (traditionell; Hongkong, Taiwan)
- Kroatisch (Kroatien)
- Tschechisch (Tschechien; QWERTY)
- Dänisch (Dänemark)
- Niederländisch (Niederlande)
- Englisch (USA)
- Englisch (Großbritannien)
- Englisch (USA, International)
- Estnisch (Estland)
- Finnisch (Finnland)
- Französisch (Belgien)
- Französisch (Kanada)
- Französisch (Frankreich)
- Französisch (Schweiz)
- Deutsch (Deutschland/Österreich)
- Deutsch (IBM)
- Deutsch (Schweiz)
- Hebräisch (Israel)
- Ungarisch (Ungarn)
- Ungarisch (Ungarn; 101 Tasten)
- Isländisch (Island)
- Irisch (Irland)
- Italienisch (Italien)
- Italienisch (Italien; 142 Tasten)
- Japanisch (Japan)
- Koreanisch (Korea)
- Norwegisch (Norwegen)
- Polnisch (Polen; Programmierer)
- Polnisch (Polen; 214-Tastatur)
- Portugiesisch (Brasilien; ABNT-Tastaturen)
- Portugiesisch (Brasilien; ABNT2-Tastaturen)
- Portugiesisch (Portugal)
- Rumänisch (Rumänien)
- Russisch (Russland; Kyrillisch)

- Serbisch (Serbien und Montenegro; Kyrillisch)
- Serbisch (Serbien und Montenegro; Lateinisch)
- Slowakisch (Slowakei)
- Slowenisch (Slowenien)
- Spanisch (Spanien)
- Spanisch (Lateinamerika)
- Spanisch (Variation)
- Schwedisch (Schweden)
- Türkisch (Türkei; F)
- Türkisch (Türkei; Q)
- Ukrainisch (Ukraine)

Bei den verschiedenen Tastaturlayouts können Zeichen unterschiedlichen Tasten zugeordnet sein. Dies kann bei der Eingabe der Passphrase zu Problemen führen. Wählen Sie das Tastaturlayout aus, das Ihrer Tastatur am besten entspricht, und verwenden Sie dieses Tastaturlayout unbedingt für jede Authentifizierung.

So wählen Sie ein Tastaturlayout aus

1. Führen Sie einen Start oder einen Neustart des Systems mit dem Laufwerk bzw. der Partition aus, die mit PGP Whole Disk Encryption geschützt ist. Beim Systemstart wird der PGP BootGuard-Anmeldebildschirm angezeigt.
2. Drücken Sie auf der Tastatur die Nach-unten-Taste, bis **Tastatur** markiert ist.
3. Drücken Sie die **Eingabetaste**. Der Bildschirm „Tastaturlayouts“ wird angezeigt.
4. Drücken Sie die **Tabulatortaste**, um zur Liste mit den Tastaturlayouts zu wechseln, und wählen Sie das gewünschte Layout mit der Nach-oben- bzw. Nach-unten-Taste aus.
5. Drücken Sie erneut die **Tabulatortaste**. Die Option **Zurück** wird markiert.
6. Drücken Sie die **Eingabetaste**. Der erweiterte PGP BootGuard-Anmeldebildschirm wird angezeigt.

Einzelanmeldung mit PGP Whole Disk Encryption verwenden

Mithilfe der Einzelanmeldung können Sie sich mit dem Windows-Kennwort gleichzeitig beim mit PGP Whole Disk Encryption verschlüsselten Laufwerk authentifizieren und bei Windows anmelden.

Funktionsweise der Einzelanmeldung

Die Einzelanmeldungsfunktion nutzt eine der Methoden, die von Microsoft Windows für das Anpassen der Windows-Anmeldung bereitgestellt werden. PGP Whole Disk Encryption verwendet die konfigurierten Anmeldeinformationen, um dynamisch bestimmte Registrierungsdatenbankeinträge zu erstellen, wenn Sie sich anmelden.

Hinweis: Das Windows-Kennwort wird *niemals* weder in der Registrierungsdatenbank noch in irgendeiner Form (verschlüsselt oder als Klartext) auf der Festplatte gespeichert.

Voraussetzungen für die Verwendung der Einzelanmeldung

- PGP Whole Disk Encryption muss installiert sein.

Lokale Benutzer und die Einzelanmeldung

Wenn ein Computer nicht Mitglied einer Domäne ist, deaktiviert PGP Whole Disk Encryption automatisch bestimmte Benutzerzugriffsfunktionen, wenn einem Laufwerk ein Einzelanmeldungsbenutzer hinzugefügt wird. Dazu zählt beispielsweise die Verwendung des Begrüßungsbildschirms sowie der schnelle Benutzerwechsel, der vom Begrüßungsbildschirm abhängig ist. Dadurch wird das Dialogfeld „Windows-Sicherheit“ verfügbar, wenn der Benutzer die Tastenkombination STRG+ALT+ENTF drückt.

Diese Funktionen sind bereits automatisch deaktiviert, wenn ein Computer Mitglied einer Domäne ist.

Laufwerk für die Verwendung der Einzelanmeldung verschlüsseln

▸ **So verschlüsseln Sie das Laufwerk für die Verwendung der Einzelanmeldung**

1. Klicken Sie auf das Bedienfeld für PGP Disk und wählen Sie **Gesamte Festplatte verschlüsseln** aus.
2. Wählen Sie das Laufwerk oder die Partition aus, das bzw. die Sie verschlüsseln möchten, und wählen Sie bei Bedarf die gewünschten PGP Whole Disk Encryption-Optionen aus. Weitere Informationen zu diesen Optionen finden Sie unter *Verschlüsselungsoptionen festlegen* (auf Seite 170).
3. Wählen Sie im Bereich **Benutzerzugriff** die Option **Neuer Passphrasenbenutzer** aus.
4. Wählen Sie **Windows-Kennwort verwenden** aus und klicken Sie auf **Weiter**.

5 Geben Sie Ihr Windows-Anmeldekennwort ein und klicken Sie auf **Beenden**.

PGP Whole Disk Encryption überprüft, ob Ihr Name in der gesamten Domäne korrekt ist und ob das Windows-Kennwort korrekt ist. Darüber hinaus überprüft PGP Whole Disk Encryption Ihr Kennwort auf unzulässige Zeichen. Sollte das Kennwort unzulässige Zeichen enthalten, dürfen Sie nicht fortfahren. Weitere Informationen zu zulässigen Zeichen finden Sie unter *Unterstützte Zeichen für Passphrasen für PGP Whole Disk Encryption* (siehe "Unterstütze Zeichen für Passphrasen für PGP Whole Disk Encryption" auf Seite 178).

6 Klicken Sie auf **Verschlüsseln** und dann auf **OK**.

Mehrere Benutzer und die Einzelanmeldung

Sie können bis zu 28 Benutzer für die Einzelanmeldung konfigurieren. Die PGP Corporation empfiehlt jedoch, die Anzahl der Einzelanmeldungsbenutzer auf möglichst wenige Personen zu beschränken, die das System gemeinsam verwenden. Obwohl es technisch möglich ist, dass eine große Anzahl von Benutzern einen einzelnen verschlüsselten Computer gemeinsam nutzt, ist dies keine sichere Lösung und die PGP Corporation rät von diesem Vorgehen ab.

Hinweis: Die Einzelanmeldungsfunktion kann nur mit Passphrasen genutzt werden. Die Einzelanmeldung kann weder mit Benutzerschlüsseln verwendet werden noch ist sie mit Smartcards oder Token kompatibel.

Mit Einzelanmeldung anmelden

Nach der Konfiguration der Einzelanmeldung wird nach dem Systemstart der PGP BootGuard-Bildschirm angezeigt. Wenn Sie den richtigen Benutzernamen und das entsprechende Kennwort eingeben, meldet PGP Whole Disk Encryption Sie bei der Windows-Sitzung an und ermöglicht Ihnen den Zugriff auf die Laufwerkspartitionen, die mit PGP Whole Disk Encryption verschlüsselt sind.

Passphrase für die Einzelanmeldung ändern

Damit Sie Windows-Kennwortänderungen mit PGP Whole Disk Encryption synchronisieren können, ist eine Änderung des Kennworts für die Einzelanmeldung im Dialogfeld „Windows-Sicherheit“ über die Option **Kennwort ändern** erforderlich. Drücken Sie hierzu die Tastenkombination STRG+ALT+ENTF.

So ändern Sie die Passphrase

1 Drücken Sie STRG+ALT+ENTF.

2 Geben Sie das alte Kennwort ein.

3 Geben Sie das neue Kennwort ein und bestätigen Sie es.

4 Klicken Sie auf **OK**.

Die Einzelanmeldung wird automatisch und transparent mit diesem neuen Kennwort synchronisiert. Sie können das neue Kennwort sofort bei der nächsten Anmeldung verwenden.

Achtung: Wenn Sie das Kennwort auf eine andere Weise ändern, z. B. über den Domänencontroller, die Windows-Systemsteuerung, den Systemadministrator oder ein anderes System, schlägt Ihre nächste Anmeldung im PGP BootGuard-Bildschirm fehl. Sie müssen in diesem Fall das alte Windows-Kennwort eingeben. Nach der erfolgreichen Anmeldung mit dem alten Windows-Kennwort im PGP BootGuard-Bildschirm wird das Windows-Anmeldefenster zur Eingabe von Benutzernamen und Kennwort angezeigt. Dort müssen Sie sich dann erfolgreich mit dem neuen Windows-Kennwort anmelden. Zu diesem Zeitpunkt wird PGP Whole Disk Encryption mit dem neuen Kennwort synchronisiert.

Dialogfeld für die Windows-Anmeldung anzeigen

Wenn Sie PGP Whole Disk Encryption mit der Einzelanmeldung (SSO) verwenden, werden Sie nach der erfolgreichen Eingabe der Passphrase im PGP BootGuard-Bildschirm automatisch am Computer angemeldet. Nach dem Start von Windows wird der Windows-Desktop angezeigt.

Unter Umständen ist es jedoch möglich, dass Sie sich über das Dialogfeld für die Windows-Anmeldung anmelden müssen, anstatt automatisch angemeldet zu werden. Eventuell müssen Sie beispielsweise auf bestimmte Netzwerkdialogfelder (z. B. das VPN des Unternehmens) zugreifen, die bei Verwendung der Einzelanmeldung umgangen werden.

So umgehen Sie die PGP Whole Disk Encryption-Funktion zum einmaligen Anmelden und zeigen das Dialogfeld für die Windows-Anmeldung an

1 Melden Sie sich wie gewohnt im PGP BootGuard-Bildschirm am Computer an, indem Sie die Passphrase eingeben und die Eingabetaste drücken.

2 Wenn der Begrüßungsbildschirm von Microsoft Windows angezeigt wird, halten Sie die Umschalttaste gedrückt, bis das Dialogfeld für die Windows-Anmeldung angezeigt wird. Beachten Sie, dass Sie die Umschalttaste beim Begrüßungsbildschirm drücken können, wenn der Windows-Startvorgang etwa zur Hälfte abgeschlossen ist.

3 Wenn das Dialogfeld für die Windows-Anmeldung angezeigt wird, geben Sie die Informationen zur Anmeldung am System ein.

Schutz von Laufwerken aufrechterhalten

In den folgenden Abschnitten wird das Arbeiten mit Laufwerken beschrieben, die mit PGP Whole Disk Encryption verschlüsselt wurden.

Laufwerks- und Partitionsinformationen abrufen

So zeigen Sie auf dem erweiterten PGP BootGuard-Anmeldebildschirm Informationen zu schreibgeschützten Laufwerken und Partitionen an

1. Führen Sie einen Start oder einen Neustart des Systems aus, auf dem ein Laufwerk oder eine Partition mit PGP Whole Disk Encryption verschlüsselt ist. Beim Systemstart wird der PGP BootGuard-Anmeldebildschirm angezeigt.
2. Drücken Sie auf der Tastatur die Nach-unten-Taste. In der rechten unteren Ecke wird **Erweitert** hervorgehoben.
3. Drücken Sie die **Eingabetaste**. Der erweiterte PGP BootGuard-Anmeldebildschirm wird angezeigt.

   In diesem Bildschirm werden folgende Informationen angezeigt:

   - Alle Laufwerke und Partitionen des Systems, einschließlich des Verschlüsselungsstatus von Laufwerken und Partitionen, die mit PGP Whole Disk Encryption verschlüsselt sind
   - Der Computername
   - Die Computer-ID
   - Das aktuell ausgewählte Laufwerk bzw. die aktuell ausgewählte Partition mit einem Vermerk, ob die Umgehungsfunktion für das ausgewählte Laufwerk bzw. die ausgewählte Partition verfügbar ist (Die Funktion „Umgehen“ kann nur von Benutzern mit Administratorrechten für das jeweilige System verwendet werden und nur, wenn dies gemäß der PGP Universal Server-Richtlinie zulässig ist.)
4. Kehren Sie zum PGP BootGuard-Anmeldebildschirm zurück, indem Sie unten rechts im Bildschirm die Option **Zurück** markieren und dann die **Eingabetaste** drücken.

Systempartition ändern

Nehmen Sie an der Systempartition auf einem mit PGP Whole Disk Encryption verschlüsselten Startlaufwerk keine Änderungen vor, da sie andernfalls beim nächsten Systemstart fehlerhaft gestartet wird. Wenn die Partition eines verschlüsselten Laufwerks geändert werden muss, entschlüsseln Sie es zunächst und nehmen danach die Änderungen vor.

Die Funktion „Umgehen“ verwenden

Hinweis: Diese Funktion kann nur von Benutzern mit Administratorrechten für das jeweilige System verwendet werden und nur, wenn dies gemäß der PGP Universal Server-Richtlinie zulässig ist.

Mit der Funktion „Umgehen“ können Sie die Authentifizierung beim Systemstart überspringen. Wenn nicht das Startlaufwerk bzw. die Startpartition, sondern eine andere Festplatte oder Partition des Systems mit PGP Whole Disk Encryption verschlüsselt ist, wird beim Systemstart der PGP BootGuard-Anmeldebildschirm angezeigt. Die Funktion „Umgehen“ ermöglicht Ihnen, die Authentifizierung zu überspringen, damit das Startlaufwerk oder die Startpartition gestartet werden kann.

Achtung: Sie können die Funktion „Umgehen“ nur verwenden, wenn das Startlaufwerk bzw. die Startpartition *nicht* mit PGP Whole Disk Encryption geschützt ist. Ist das Startlaufwerk bzw. die Startpartition jedoch geschützt und Sie umgehen die Authentifizierung, wird das Betriebssystem nicht geladen und der Computer fährt nicht hoch.

So verwenden Sie die Funktion „Umgehen“

1. Führen Sie einen Start bzw. einen Neustart des Systems durch, auf dem das Laufwerk bzw. die Partition mit PGP Whole Disk Encryption geschützt ist. Beim Systemstart wird der PGP BootGuard-Anmeldebildschirm angezeigt.
2. Drücken Sie auf der Tastatur die Nach-unten-Taste. In der rechten unteren Ecke wird „Erweitert“ hervorgehoben.
3. Drücken Sie die **Eingabetaste**. Der erweiterte PGP BootGuard-Anmeldebildschirm wird angezeigt.
4. Drücken Sie auf der Tastatur erneut die Nach-unten-Taste. In der rechten unteren Ecke wird **Umgehen** hervorgehoben.
5. Drücken Sie die **Eingabetaste**. Der erweiterte PGP BootGuard-Anmeldebildschirm wird nicht mehr angezeigt und der Systemstart läuft normal ab.

Andere Benutzer zu verschlüsselten Laufwerken oder Partitionen hinzufügen

Der Benutzer, der ein verschlüsseltes Laufwerk oder eine verschlüsselte Partition erstellt, kann das Laufwerk bzw. die Partition anderen Benutzern zugänglich machen. Diese zusätzlichen Benutzer können dann mit ihrer eigenen eindeutigen Passphrase bzw. ihrem eigenen privaten Schlüssel oder Token (einschließlich PIV-Karten) auf das verschlüsselte Laufwerk bzw. die verschlüsselte Partition zugreifen. Pro verschlüsseltem Laufwerk können Sie bis zu 120 Benutzer hinzufügen.

Wenn Sie ermitteln möchten, welcher Benutzertyp dem verschlüsselten Laufwerk zugeordnet ist, zeigen Sie mit der Maus auf den Namen des Benutzers in der Liste „Benutzerzugriff". Der Benutzertyp wird in einer Art Tipp angezeigt. Ein Token-Schlüsselsymbol zeigt einen Token-Benutzer an. Für einen Einzelanmeldungsbenutzer werden die Windows-Domäne und der Benutzername angegeben.

Achtung: Wenn mehrere Benutzer auf mit PGP Whole Disk Encryption geschützte Laufwerke bzw. Partitionen zugreifen können, ist gewährleistet, dass der Zugriff im Fall eines Verlusts der Passphrase oder des Authentifizierungs-Tokens weiterhin möglich ist. Benutzer, die für verschlüsselte Laufwerke oder Partitionen konfiguriert sind, können sich im Anmeldebildschirm von PGP Whole Disk Encryption authentifizieren und dann jedes geschützte Laufwerk bzw. jede geschützte Partition im System entsperren.

So fügen Sie Laufwerken oder Partitionen, die mit PGP Whole Disk Encryption geschützt sind, weitere Benutzer hinzu

1. Klicken Sie links im Hauptbildschirm von PGP Desktop auf das Bedienfeld für PGP Disk.
2. Wählen Sie in der Laufwerksliste oben im Arbeitsbereich von PGP Disk das verschlüsselte Laufwerk oder die verschlüsselte Partition aus, für das bzw. die Sie weitere Benutzer hinzufügen möchten.
3. Klicken Sie auf **Neuer Passphrasenbenutzer**. Das Dialogfeld „Benutzertyp auswählen" wird angezeigt.
4. Folgen Sie den Anleitungen, die unter *Laufwerk verschlüsseln* (auf Seite 179) im Schritt „Benutzerzugriff" aufgeführt sind.

Hinweis: Die Verschlüsselung mit öffentlichen Schlüsseln zählt aus folgenden Gründen zu den sichersten Schutzmaßnahmen beim Hinzufügen von anderen Benutzern zu Laufwerken oder Partitionen, die mit PGP Whole Disk Encryption verschlüsselt sind: (1) Passphrasen müssen neuen Benutzern nicht mitgeteilt werden. Das Risiko, dass Passphrasen von unberechtigten Personen abgefangen oder zufällig mitgehört werden, ist daher sehr gering. (2) Andere Benutzer müssen sich keine weiteren Passphrasen merken. (3) Die Verwaltung einer Liste von Benutzern wird vereinfacht, wenn jeder Benutzer einen eigenen privaten Schlüssel für den Zugriff auf das Laufwerk verwendet. Wenn Sie ein Startlaufwerk oder eine Startpartition mit PGP Whole Disk Encryption schützen, muss sich der öffentliche Schlüssel auf einem Token befinden.

Benutzer von verschlüsselten Laufwerken oder Partitionen löschen

Gelegentlich kann es erforderlich sein, einem Benutzer den Zugriff auf ein verschlüsseltes Laufwerk bzw. eine verschlüsselte Partition zu entziehen.

So entfernen Sie einen Benutzer von einem verschlüsselten Laufwerk bzw. einer verschlüsselten Partition

1. Wählen Sie im Bildschirm für die Verschlüsselung der gesamten Festplatte (Partition) das mit PGP Whole Disk Encryption verschlüsselte Laufwerk bzw. die verschlüsselte Partition aus.
2. Wählen Sie in der Liste **Benutzerzugriff** den Namen des Benutzers aus, den Sie entfernen möchten.
3. Klicken Sie auf **Benutzer löschen**. Im Dialogfeld „Passphrase“ werden Sie aufgefordert, sich zu authentifizieren.
4. Geben Sie eine gültige Passphrase ein und klicken Sie auf „OK“. Der andere Benutzer wird entfernt.

Benutzer-Passphrasen ändern

Wenn Sie die Einzelanmeldung verwenden, ändern Sie das Kennwort entsprechend der Informationen unter *Passphrase bei Verwendung der Einzelanmeldung ändern* (auf Seite 198).

So ändern Sie Benutzerpassphrasen für ein verschlüsseltes Laufwerk oder eine verschlüsselte Partition

1. Wählen Sie im Bildschirm für die Verschlüsselung der gesamten Festplatte (Partition) das mit PGP Whole Disk Encryption verschlüsselte Laufwerk bzw. die verschlüsselte Partition aus.

2 Wählen Sie in der Liste **Benutzerzugriff** den Namen des Benutzers aus, dessen Passphrase Sie ändern möchten.

3 Klicken Sie auf **Passphrase ändern**. Sie werden zur Eingabe der aktuellen Passphrase aufgefordert.

4 Geben Sie die entsprechende Passphrase ein und klicken Sie auf **OK**. Das Dialogfeld „Benutzerpassphrase ändern“ wird angezeigt.

5 Geben Sie eine neue Passphrase ein.

6 Geben Sie im Feld „Passphrase bestätigen“ die neue Passphrase erneut ein und klicken Sie auf **OK**. Die Passphrase wird geändert.

Die Passphrasen-Qualitätsanzeige kann als allgemeiner Anhaltspunkt für die Stärke der erstellten Passphrase verwendet werden. Weitere Informationen finden Sie unter *Die Passphrasen-Qualitätsanzeige* (auf Seite 352).

Als zusätzliche Sicherheitsmaßnahme werden die für die Passphrase eingegebenen Zeichen in der Regel nicht auf dem Bildschirm angezeigt. Wenn die Zeichen der Passphrase während der Eingabe angezeigt werden sollen, aktivieren Sie das Kontrollkästchen Tastatureingabe anzeigen.

Passphrase bei Verwendung der Einzelanmeldung ändern

Wenn Sie die Einzelanmeldungsfunktion von PGP Whole Disk Encryption verwenden möchten, sollten Sie die Passphrase im Dialogfeld „Windows-Sicherheit“ über die Option **Kennwort ändern** ändern.

Hinweis: Sie können auf das Dialogfeld „Windows-Sicherheit“ zugreifen, indem Sie die Tastenkombination **STRG+ALT+ENTF** drücken.

So ändern Sie die Passphrase bei Verwendung der Einzelanmeldungsfunktion

1 Drücken Sie STRG+ALT+ENTF. Das Dialogfeld „Windows-Sicherheit“ wird angezeigt.

2 Geben Sie die alte Passphrase ein.

3 Geben Sie die neue Passphrase ein und bestätigen Sie sie.

4 Klicken Sie auf **OK**. Das Windows-Kennwort und die Passphrase für PGP Whole Disk Encryption werden zusammen geändert. Geben Sie die neue Passphrase bei der nächsten Anmeldung ein.

Achtung: Wenn Sie die Passphrase auf eine andere Weise als hier beschrieben ändern, können Sie sich nicht mit der neuen Passphrase im PGP BootGuard-Bildschirm anmelden. Sie müssen in diesem Fall die alte Passphrase eingeben. Nach der erfolgreichen Anmeldung im PGP BootGuard-Bildschirm mit der alten Passphrase wird das Windows-Anmeldefenster zur Eingabe von Benutzernamen und Kennwort angezeigt. Sie müssen sich dann erfolgreich über den Windows-Anmeldebildschirm anmelden. Zu diesem Zeitpunkt wird PGP Whole Disk Encryption mit der neuen Passphrase synchronisiert.

Lokale Benutzer und die Einzelanmeldungsfunktion von PGP Whole Disk Encryption

Wenn ein Computer nicht Mitglied einer Domäne ist, stellt PGP Whole Disk Encryption automatisch sicher, dass Benutzer sich unter Verwendung von STRG+ALT+ENTF anmelden müssen. Hierfür werden bestimmte Benutzerzugriffsfunktionen von Windows deaktiviert, u. a. die Option zum Verwenden des Begrüßungsbildschirms **und STRG+ALT+ENTF, nachdem ein Einzelanmeldungsbenutzer hinzugefügt wurde.**

Diese Funktionen sind automatisch aktiviert, wenn ein Computer Mitglied einer Domäne ist.

Verschlüsselte Laufwerke oder Partitionen umschlüsseln

Ziehen Sie die Umschlüsselung von geschützten Laufwerken bzw. Partitionen in Betracht, wenn eine Passphrase oder ein Authentifizierungs-Token eventuell in die falschen Hände geraten ist oder wenn Benutzer entfernt wurden, die zuvor über Zugriff verfügten.

PGP Whole Disk Encryption verwendet für die Umschlüsselung von Laufwerken oder Partitionen zwar denselben Verschlüsselungsalgorithmus (AES-256), jedoch einen anderen zugrunde liegenden Verschlüsselungsschlüssel. Dieses Verfahren kann mit dem Entschlüsseln und erneuten Verschlüsseln von Laufwerken bzw. Partitionen verglichen werden, jedoch ist der Vorgang wesentlich schneller.

Hinweis: Die Umschlüsselung gilt für alle bereits verschlüsselten Partitionen. Wenn Sie eine zu verschlüsselnde Partition auswählen, bedeutet dies implizit, dass alle Partitionen auf demselben Laufwerk, die bereits verschlüsselt sind, ebenfalls nacheinander umgeschlüsselt werden.

So schlüsseln Sie verschlüsselte Laufwerke bzw. Partitionen um

1. Wählen Sie das entsprechende verschlüsselte Laufwerk bzw. die Partition aus.
2. Klicken Sie auf **Laufwerk > Umschlüsseln**. Sie werden zur Authentifizierung aufgefordert.
3. Geben Sie die entsprechende Passphrase ein und klicken Sie auf **OK**. Der Umschlüsselungsvorgang wird gestartet.

Vorgehensweise bei vergessenen Passphrasen

Falls Sie Ihre Passphrase vergessen haben und das System entsprechend konfiguriert wurde, können Sie PGP BootGuard umgehen, indem Sie drei von fünf Sicherheitsfragen richtig beantworten. Sie haben die fünf Sicherheitsfragen erstellt und beantwortet. Dies ähnelt der Wiederherstellung Ihres Schlüssels, wenn Sie ihn verloren oder die Passphrase für den Schlüssel vergessen haben.

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung verwenden, hat der PGP Universal Server-Administrator möglicherweise die Option für die lokale Selbstwiederherstellung deaktiviert. Der Administrator kann auch festgelegt haben, dass die lokale Selbstwiederherstellung bei der Anmeldung konfiguriert wird. In diesem Fall werden Sie aufgefordert, die Sicherheitsfragen beim Einrichten von PGP Desktop einzugeben.

So erstellen Sie Sicherheitsfragen

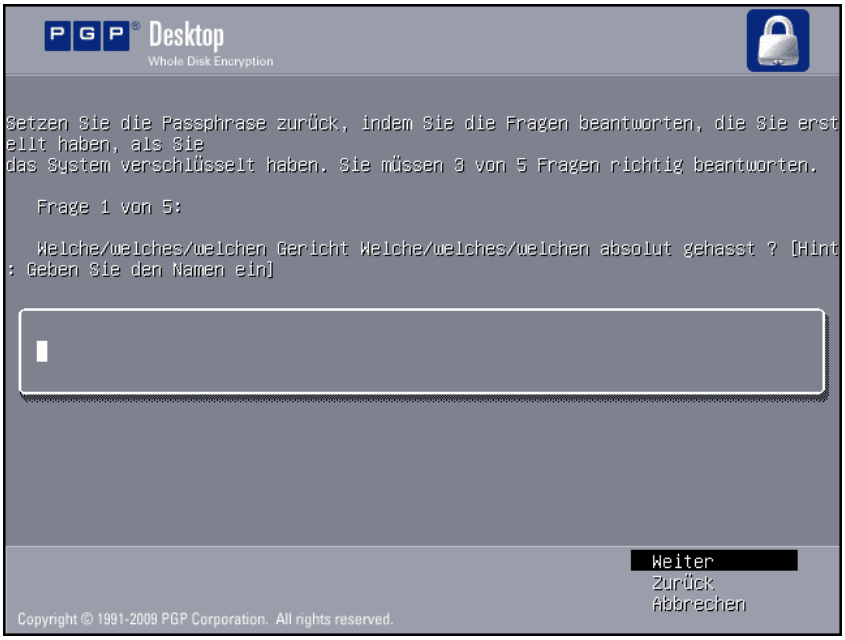
1. Verschlüsseln Sie das interne Laufwerk mit PGP Desktop. Sie können entweder einen Passphrasenbenutzer oder einen Windows-Einzelanmeldungsbenutzer verwenden.
2. Klicken Sie in PGP Desktop mit der rechten Maustaste auf den Namen des Benutzers und wählen Sie die Option **Sicherheitsfragen hinzufügen** aus.

   Hinweis: Sie können keine Sicherheitsfragen für den WDE-Administrator oder den ADK erstellen.
3. Erstellen und beantworten Sie die fünf Sicherheitsfragen. Der Name des Benutzers wird angezeigt. Rechts neben dem Namen steht **LSR** (sowie eine Quickinfo). Dies zeigt an, dass die lokale Selbstwiederherstellung für den Benutzer konfiguriert ist.

So stellen Sie die Passphrase im PGP BootGuard-Bildschirm wieder her

1. Wählen Sie im PGP BootGuard-Bildschirm mit den Pfeiltasten die Option **Passphrase vergessen** aus und drücken Sie die Eingabetaste.

2 Beantworten Sie die erste angezeigte Sicherheitsfrage. Geben Sie die Antwort ein und drücken Sie die Eingabetaste.


PGP Desktop
Whole Disk Encryption
Setzen Sie die Passphrase zurück, indem Sie die Fragen beantworten, die Sie erst
ellt haben, als Sie
das System verschlüsselt haben. Sie müssen 3 von 5 Fragen richtig beantworten.
Frage 1 von 5:
Welche/welches/welchen Gericht Welche/welches/welchen absolut gehasst ? [Hint
: Geben Sie den Namen ein]
Weiter
Zurück
Abbrechen
Copyright © 1991-2009 PGP Corporation. All rights reserved.

3 Fahren Sie mit der Beantwortung der Fragen fort. Sie müssen drei der fünf Fragen richtig beantworten.

4 Wenn Sie die Fragen richtig beantwortet haben, wird das Windows-Betriebssystem gestartet. Wenn das Dialogfeld für die Anmeldung bei Windows angezeigt wird, geben Sie Ihren Windows-Anmeldenamen und Ihr Kennwort ein.

Wenn Windows hochgefahren ist, wird das Dialogfeld „PGP Disk – Benutzerpassphrase ändern“ angezeigt.

5 Geben Sie eine neue Passphrase für den Benutzer ein und bestätigen Sie diese. Klicken Sie auf **OK**. Die neue Passphrase wird für den Benutzer erstellt.

Die Passphrasen-Qualitätsanzeige kann als allgemeiner Anhaltspunkt für die Stärke der erstellten Passphrase verwendet werden. Weitere Informationen finden Sie unter *Die Passphrasen-Qualitätsanzeige* (auf Seite 352).

Als zusätzliche Sicherheitsmaßnahme werden die für die Passphrase eingegebenen Zeichen in der Regel nicht auf dem Bildschirm angezeigt. Wenn die Zeichen der Passphrase während der Eingabe angezeigt werden sollen, aktivieren Sie das Kontrollkästchen **Tastatureingabe anzeigen.**

Sollten Sie die Passphrase wieder vergessen, werden dieselben Sicherheitsfragen angezeigt. Wenn Sie die Sicherheitsfragen ändern möchten, klicken Sie mit der rechten Maustaste auf den Benutzernamen und wählen Sie **Sicherheitsfragen erstellen** aus.

Sicherungskopien erstellen und Daten wiederherstellen

Während die meisten Sicherungsprogramme die Daten auf einem mit PGP Whole Disk Encryption verschlüsselten Laufwerk sichern können, treten bei einigen Sicherungsprogrammen Probleme auf. Bei diesen Sicherungsprogrammen kommt es zu Problemen, wenn die Datei „PGPWDE01“ auftritt (eine von PGP Whole Disk Encryption verwendete Datei). Als Lösung können Sie bei diesen Programmen die Datei „PGPWDE01“ von der Sicherung ausschließen (bei den meisten Sicherungsprogrammen ist der Ausschluss einzelner Dateien möglich). Wenn Sie eine Sicherungskopie mit diesen Programmen erstellt haben, sollten Sie prüfen, ob diese Sicherungskopie funktioniert.

Automatische Sicherungssoftware auf einem mit PGP Whole Disk Encryption verschlüsselten Laufwerk verwenden

Sie können Laufwerke oder Partitionen, die mit PGP Whole Disk Encryption geschützt sind, automatisch sichern. Sichern Sie das System, bevor Sie es mit PGP Whole Disk Encryption verschlüsseln.

Beachten Sie, dass Dateien, die von der Software gesichert werden, zunächst entschlüsselt werden. Wenn Sie verschlüsselte Daten sichern möchten, verwenden Sie durch PGP Virtual Disk oder PGP NetShare geschützte Ordner.

PGP Desktop von verschlüsselten Laufwerken oder Partitionen deinstallieren

Wenn auf einem System Laufwerke oder Partitionen mit PGP Whole Disk Encryption geschützt sind und PGP Desktop deinstalliert wird, ist der Zugriff auf diese Laufwerke oder Partitionen nicht mehr möglich. Aus diesem Grund wird durch eine Sicherheitsfunktion die Deinstallation von PGP Desktop verhindert, wenn auf dem System Laufwerke oder Partitionen mit PGP Whole Disk Encryption geschützt sind. In diesem Fall wird eine Fehlermeldung angezeigt, dass die Deinstallation zum Schutz der verschlüsselten Laufwerke bzw. Partitionen abgebrochen wird.

Wenn Sie PGP Desktop deinstallieren möchten, entschlüsseln Sie zunächst alle mit PGP Whole Disk Encryption geschützten Laufwerke oder Partitionen.

Mit Wechseldatenträgern arbeiten

In diesem Abschnitt wird das Arbeiten mit Wechseldatenträgern beschrieben. Wenn Sie PGP Whole Disk Encryption in einer von einem PGP Universal Server verwalteten Umgebung verwenden, kann es aufgrund Ihrer Sicherheitsrichtlinie erforderlich sein, Wechseldatenträger zu verschlüsseln. Aufgrund Ihrer Sicherheitsrichtlinie kann es ferner erforderlich sein, dass Wechseldatenträger als schreibgeschützte Laufwerke aktiviert werden, jedoch ist eine Option zum Verschlüsseln des Laufwerks verfügbar.

Achtung: Verwenden Sie immer die Option **Hardware sicher entfernen** in Microsoft Windows, um angeschlossene USB-Geräte vor dem Trennen anzuhalten.

Wechseldatenträger verschlüsseln

Wenn Sie PGP Whole Disk Encryption in einer von einem PGP Universal Server verwalteten Umgebung verwenden, kann es aufgrund Ihrer Sicherheitsrichtlinie erforderlich sein, Wechseldatenträger zu verschlüsseln. Wenn Sie den Wechseldatenträger einlegen, wird das Dialogfeld „PGP Desktop – Speichergerät angeschlossen“ angezeigt.

Führen Sie einen der folgenden Schritte aus:

- Wenn der Wechseldatenträger ein externes Laufwerk ist, z. B. ein USB-Flash-Laufwerk oder eine externe Festplatte, klicken Sie auf **Verschlüsseln**. Das Gerät wird automatisch an Ihren Schlüssel verschlüsselt. Wenn das Startlaufwerk mit Schlüsseln von anderen Benutzern verschlüsselt ist, werden diese Schlüssel dem Wechseldatenträger als Benutzer hinzugefügt. Wenn Ihr Schlüssel nicht gefunden wird kann oder wenn die Schlüssel anderer Benutzer nicht gefunden werden können, werden Sie aufgefordert, einen Passphrasenbenutzer zu erstellen.

  Hinweis: Wenn der PGP Universal Server-Administrator festgelegt hat, dass alle Wechseldatenträger automatisch verschlüsselt werden, das Startlaufwerk jedoch nicht verschlüsselt ist, wird das erste Schlüsselpaar am Schlüsselbund des Benutzers zum Verschlüsseln des Geräts verwendet.

  Abhängig von der Größe des Laufwerks kann der Abschluss des Verschlüsselungsvorgangs einige Zeit dauern. Der Wechseldatenträger kann während der Verschlüsselung weiterhin verwendet werden.

  Warnung: Stellen Sie sicher, dass der Verschlüsselungsvorgang abgeschlossen ist, bevor Sie das Laufwerk entfernen.

- Wenn Sie das Gerät nicht verschlüsseln möchten, klicken Sie auf **Sperren**. Das Gerät ist dann gesperrt und schreibgeschützt. Wenn Sie versuchen, eine Datei auf dem Gerät zu ändern oder davon zu löschen, wird eine Windows-Fehlermeldung angezeigt.

  Wenn der Wechseldatenträger ein Musikgerät oder eine Digitalkamera ist, klicken Sie auf **Sperren**. Diese Art von Geräten funktioniert nicht, wenn ihr Inhalt verschlüsselt ist. Falls Sie versehentlich ein Musikgerät oder eine Digitalkamera verschlüsseln, müssen Sie das Gerät zunächst wieder entschlüsseln. Abhängig von den Sicherheitsrichtlinien Ihres Unternehmens müssen Sie sich eventuell an die IT-Abteilung oder an den PGP-Administrator wenden, um Unterstützung bei der Entschlüsselung des Geräts zu erhalten.

Wenn gemäß der Sicherheitsrichtlinien alle Wechseldatenträger verschlüsselt sein müssen und der PGP Universal Server nicht verfügbar ist (wenn Sie beispielsweise im Flugzeug sind und keine Verbindung zum Unternehmensnetzwerk besteht), kann der Wechseldatenträger nicht verschlüsselt werden. Das Gerät ist in diesem Fall gesperrt und schreibgeschützt. Wenn Sie das nächste Mal eine Verbindung mit dem PGP Universal Server herstellen, können Sie den Inhalt des Laufwerks verschlüsseln (sofern er nicht bereits verschlüsselt ist).

Hinweis: Wenn der PGP-Administrator festgelegt hat, dass alle Wechseldatenträger verschlüsselt sein müssen, ist die Option **PGP-Dienste beenden** im Menü des PGP-Symbols im Infobereich der Taskleiste nicht mehr verfügbar.

Gesperrte (schreibgeschützte) Laufwerke im schreibgeschützten Modus verwenden

Wenn Sie PGP Whole Disk Encryption in einer von einem PGP Universal Server verwalteten Umgebung verwenden, kann es aufgrund Ihrer Sicherheitsrichtlinie erforderlich sein, Wechseldatenträger als schreibgeschützte Geräte zu aktivieren. Wenn Sie den Wechseldatenträger einlegen, wird das Dialogfeld „PGP Desktop – Speichergerät angeschlossen“ angezeigt. Der Wechseldatenträger ist gesperrt und Sie können erst Daten auf den Datenträger schreiben, wenn Sie ihn verschlüsseln. Wenn Sie das Gerät verschlüsseln, können Sie den Datenträger wie gewohnt verwenden.

Führen Sie einen der folgenden Schritte aus:

- Wenn es sich beim Wechseldatenträger um ein externes Laufwerk handelt (z. B. ein USB-Flash-Laufwerk oder eine externe Festplatte) und Sie auf das Laufwerk schreiben möchten, klicken Sie auf **Verschlüsseln**. Das Gerät wird automatisch an Ihren Schlüssel verschlüsselt. Wenn das Startlaufwerk mit Schlüsseln von anderen Benutzern verschlüsselt ist, werden diese Schlüssel dem Wechseldatenträger als Benutzer hinzugefügt. Wenn Ihr Schlüssel nicht gefunden wird kann oder wenn die Schlüssel anderer Benutzer nicht gefunden werden können, werden Sie aufgefordert, einen Passphrasenbenutzer zu erstellen.

Abhängig von der Größe des Laufwerks kann der Abschluss des Verschlüsselungsvorgangs einige Zeit dauern. Der Wechseldatenträger kann während der Verschlüsselung weiterhin verwendet werden.

Warnung: Stellen Sie sicher, dass der Verschlüsselungsvorgang abgeschlossen ist, bevor Sie das Laufwerk entfernen.

- Wenn Sie das Gerät nicht verschlüsseln möchten, klicken Sie auf **Sperren**. Das Gerät ist dann gesperrt und schreibgeschützt. Wenn Sie versuchen, eine Datei auf dem Gerät zu ändern oder davon zu löschen, wird eine Windows-Fehlermeldung angezeigt.

  Wenn der Wechseldatenträger ein Musikgerät oder eine Digitalkamera ist, klicken Sie auf **Sperren**. Diese Art von Geräten funktioniert nicht, wenn ihr Inhalt verschlüsselt ist. Falls Sie versehentlich ein Musikgerät oder eine Digitalkamera verschlüsseln, müssen Sie das Gerät zunächst wieder entschlüsseln. Abhängig von den Sicherheitsrichtlinien Ihres Unternehmens müssen Sie sich eventuell an die IT-Abteilung oder an den PGP-Administrator wenden, um Unterstützung bei der Entschlüsselung des Geräts zu erhalten.

Wechseldatenträger auf anderen Systemen verwenden

Wenn Sie einen Wechseldatenträger (z. B. ein USB-Flash-Laufwerk) mit PGP Whole Disk Encryption schützen, können Sie diesen Wechseldatenträger auf einem anderen Windows- oder Mac OS X-System verwenden und auf diesem anderen System auf die verschlüsselten Dateien auf dem Datenträger zugreifen. Auf mit PGP Whole Disk Encryption unter Linux erstellte Wechseldatenträger kann mit PGP Desktop Version 10.0 oder höher zugegriffen werden.

Sie müssen eine Authentifizierung durchführen, um auf den Inhalt des Datenträgers zuzugreifen.

Hinweis: Beachten Sie die PGP Desktop-Lizenzierung, wenn Sie einen verschlüsselten Wechseldatenträger auf einem anderen System verwenden. Sie benötigen zum Schützen eines Datenträgers mit PGP Whole Disk Encryption die entsprechende PGP Desktop-Lizenz. Wenn Sie jedoch einen Wechseldatenträger mit PGP Whole Disk Encryption verschlüsselt haben, können Sie diesen Wechseldatenträger auf einem anderen Computer mit PGP Desktop 9.5.2 oder höher auch dann verwenden, wenn dieser Computer nicht über eine PGP Desktop-Lizenz für PGP Whole Disk Encryption verfügt.

Verschlüsselte Wechseldatenträger neu formatieren

Wenn Sie einen Wechseldatenträger verschlüsselt und dann mit der Windows-Datenträgerverwaltung neu formatiert haben, werden Sie zur Eingabe der Passphrase aufgefordert, wenn Sie den Datenträger das nächste Mal einlegen.

Führen Sie folgende Schritte aus, damit dieses Vorgehen nicht erforderlich ist:

1. Rufen Sie eine Eingabeaufforderung auf (**Start > Ausführen** und geben Sie `cmd` ein) und wechseln Sie zum Ordner `C:\Programme\PGP Corporation\PGP Desktop`.
2. Geben Sie folgenden Befehl ein:

   ```
   pgpwde --fixmbr --disk 1
   ```

   Wenn auf dem System mehrere verschlüsselte Laufwerke vorhanden sind, müssen Sie ggf. zunächst den Befehl `pgpwde --enum` ausführen. Mit diesem Befehl wird eine Liste der verschlüsselten Laufwerke angezeigt. Wenn nach diesem Befehl die Information zurückgegeben wird, dass es sich beim USB-Laufwerk nicht um Laufwerk 1 handelt, verwenden Sie stattdessen die entsprechende Nummer (wenn das USB-Laufwerk beispielsweise Laufwerk 2 ist, geben Sie den Befehl `pgpwde --fixmbr --disk 2` ein, um die Verschlüsselung zu entfernen).

Danach werden Sie beim Einlegen des Datenträgers nicht mehr zur Eingabe der Passphrase aufgefordert.

PGP Whole Disk Encryption in einer von einem PGP Universal Server verwalteten Umgebung verwenden

PGP Whole Disk Encryption kann für Benutzer von PGP Desktop verwaltet werden, die in einer von einem PGP Universal Server verwalteten Umgebung arbeiten. Administratoren können Benutzern in ihrem Unternehmen Installationsprogramme für PGP Desktop bereitstellen.

PGP Whole Disk Encryption verwalten

Der PGP-Administrator kann Folgendes steuern:

- **Die Verfügbarkeit der PGP Whole Disk Encryption-Funktion für Benutzer**. Wenn Sie in einer von einem PGP Universal Server verwalteten Umgebung arbeiten und die PGP Whole Disk Encryption-Funktion *nicht* verfügbar ist, erkundigen Sie sich beim PGP-Administrator, ob die Funktion durch eine Richtlinie deaktiviert wurde.

  Für die PGP Whole Disk Encryption-Funktion ist außerdem eine entsprechende Lizenz von der PGP Corporation erforderlich. Wenn die Funktion für Sie deaktiviert ist, obwohl sie durch eine Richtlinien aktiviert wurde, wenden Sie sich an den PGP-Administrator, um sicherzustellen, dass Sie über eine entsprechende Lizenz verfügen.

- **Die Möglichkeit der Wiederherstellung von Laufwerken oder Partitionen, die mit PGP Whole Disk Encryption geschützt sind**. Wenn Sie die Passphrase für ein mit PGP Whole Disk Encryption verschlüsseltes Laufwerk bzw. eine Partition vergessen oder wenn Sie das Authentifizierungs-Token verlieren, ist das Laufwerk oder die Partition nicht zugänglich. Wenn Sie die PGP Whole Disk Encryption-Funktion jedoch in einer von einem PGP Universal Server verwalteten Umgebung verwenden, erkundigen Sie sich beim PGP-Administrator, ob eine Laufwerks- oder Partitionswiederherstellung möglich ist.
- **Die Notwendigkeit der Verschlüsselung des Startlaufwerks mit PGP Whole Disk Encryption bei der Installation von PGP Desktop**.

  Wenn Sie mit PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung arbeiten, erhalten Sie weitere Informationen vom PGP-Administrator.
- **Die Verwendung der Einzelanmeldungsfunktion von PGP Whole Disk Encryption auf dem Computer**.

  Weitere Informationen zu dieser Funktion finden Sie unter *Einzelanmeldung mit PGP Whole Disk Encryption verwenden* (auf Seite 190).
- **Die mit der PGP Whole Disk Encryption-Funktion verwendbaren Modi**.
- **Die Verwendung eines Administratorschlüssels (mit einer Smartcard) durch den PGP-Administrator zum Zugriff auf Ihr verschlüsseltes Laufwerk bzw. Ihre verschlüsselte Partition.**

Weitere Informationen zu Verschlüsselungsmodi finden Sie unter *Authentifizierungsmethode für das Laufwerk bestimmen* (auf Seite 167).

Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung verwenden, müssen Sie das Startlaufwerk oder die Partition nach der Installation von PGP Desktop möglicherweise mit der PGP Whole Disk Encryption-Funktion verschlüsseln. Es ist auch möglich, dass die PGP Whole Disk Encryption-Funktion vom PGP-Administrator deaktiviert wurde.

Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung verwenden, werden Sie beim Einlegen eines Wechseldatenträgers möglicherweise aufgefordert, diesen zu verschlüsseln. Weitere Informationen finden Sie unter *Wechseldatenträger verschlüsseln* (auf Seite 203).

Wenn sich Ihre Richtlinien ändern sollten, insbesondere von der Möglichkeit zur Verschlüsselung eines Laufwerks zur Deaktivierung dieser Funktion, können Sie alle bereits mit Whole Disk Encryption verschlüsselten Laufwerke trotzdem weiterhin verwenden. Jedoch können Sie keine weiteren Laufwerke mehr verschlüsseln, bestehende verschlüsselte Laufwerke umschlüsseln oder neue Benutzer hinzufügen.

Weitere Informationen finden Sie unter *PGP Desktop mit PGP Universal Server verwenden* (auf Seite 357).

Wiederherstellungs-Token erstellen

Wenn Sie in einer von einem PGP Universal Server verwalteten Umgebung arbeiten und Sie entsprechend der für Sie geltenden Richtlinien Wiederherstellungs-Token für das gesamte Laufwerk erstellen können, wird von PGP Desktop immer dann ein Wiederherstellungs-Token erstellt, wenn Sie ein Laufwerk, eine Partition (unter Windows) oder einen Wechseldatenträger mit PGP Whole Disk Encryption verschlüsseln. Dieses Wiederherstellungs-Token kann zum Zugriff auf das Laufwerk oder die Partition (unter Windows) verwendet werden, falls die Passphrase oder das Authentifizierungs-Token (unter Windows) verloren gegangen ist.

Falls die für Sie geltenden Richtlinien diese Funktion nicht unterstützen oder falls Sie nicht in einer von einem PGP Universal Server verwalteten Umgebung mit einer vorkonfigurierten Installation von PGP Desktop arbeiten, können Sie keine Whole Disk-Wiederherstellungs-Token verwenden.

Dieses Wiederherstellungs-Token wird automatisch an den PGP Universal Server gesendet, der für die Verwaltung der Sicherheit des mit PGP Whole Disk Encryption geschützten Laufwerks bzw. der Partition (unter Windows) zuständig ist.

Wenn Sie in einer von einem PGP Universal Server verwalteten Umgebung arbeiten und die Passphrase oder das Authentifizierungs-Token für den Schutz eines Laufwerks oder einer Partition (unter Windows) mit PGP Whole Disk Encryption verlieren, bitten Sie den PGP-Administrator, Sie bei der Verwendung des Wiederherstellungs-Tokens zu unterstützen.

Das Wiederherstellungs-Token kann nur einmal verwendet werden, um auf ein Laufwerk oder eine Partition (unter Windows) zuzugreifen, das bzw. die mit PGP Whole Disk Encryption geschützt ist. Sobald ein Wiederherstellungs-Token verwendet wurde, wird automatisch ein neues Token erstellt und an den PGP Universal Server gesendet. Der Benutzer von PGP Desktop erhält die Möglichkeit, einen neuen Benutzer zu erstellen oder die auf dem Laufwerk bzw. der Partition vorhandenen Benutzer beizubehalten.

Beachten Sie, dass das Wiederherstellungs-Token nur verwendet wird, um auf ein verschlüsseltes Laufwerk oder eine verschlüsselte Partition (unter Windows) zuzugreifen. Das Wiederherstellungs-Token kann nicht zur Verschlüsselung oder Entschlüsselung von Daten genutzt werden.

Achtung: Wenn die Sicherheit der mit PGP Whole Disk Encryption verschlüsselten Laufwerke bzw. Partitionen (unter Windows) durch den Verlust oder die Offenlegung der Passphrase oder des Authentifizierungs-Tokens (unter Windows) beeinträchtigt ist, sollten Sie die Umschlüsselung der Laufwerke bzw. Partitionen in Betracht ziehen. Hierbei wird das Laufwerk oder die Partition mit demselben Verschlüsselungsalgorithmus umgeschlüsselt, jedoch wird ein anderer zugrunde liegender Verschlüsselungsschlüssel verwendet. Dieses Verfahren kann mit dem Entschlüsseln und erneuten Verschlüsseln von Laufwerken bzw. Partitionen verglichen werden, jedoch ist der Vorgang wesentlich schneller.

Wiederherstellungs-Token verwenden

Nachdem Sie ein Wiederherstellungs-Token vom PGP Universal-Administrator erhalten haben, führen Sie die folgenden Schritte aus, um das Laufwerk zu entsperren.

Bei der Eingabe des Wiederherstellungs-Tokens müssen Sie die Schreibweise in Bezug auf Groß-/Kleinschreibung (alles Großbuchstaben) oder Gedankenstriche, die Sie vom PGP Universal-Administrator erhalten haben, nicht einhalten. Sie können auf Wunsch nur Kleinbuchstaben ohne Gedankenstriche eingeben.

So verwenden Sie ein Wiederherstellungs-Token auf einem Startlaufwerk

- Geben Sie im PGP BootGuard-Bildschirm das Wiederherstellungs-Token in das Passphrasenfeld ein.

So verwenden Sie ein Wiederherstellungs-Token auf einem Wechseldatenträger

- Legen Sie das Laufwerk ein. Wenn Sie zur Eingabe der Passphrase aufgefordert werden, geben Sie das Wiederherstellungs-Token ein.

Daten von verschlüsselten Laufwerken wiederherstellen

In seltenen Fällen müssen Sie möglicherweise Daten von einem verschlüsselten Laufwerk wiederherstellen, das beschädigt oder zerstört wurde. Es kann auch vorkommen, dass Sie nicht über die Anmeldeinformationen zum Zugriff auf das Laufwerk verfügen (z. B. wenn das Laufwerk von einem ehemaligen Mitarbeiter verschlüsselt wurde). In diesen Fällen haben Sie mehrere Möglichkeiten:

1. Verwenden Sie einen Wiederherstellungsdatenträger. Wenn vor der Verschlüsselung des Laufwerks oder der Partition ein Wiederherstellungsdatenträger erstellt wurde, kann dieser zur Entschlüsselung des Laufwerks verwendet werden. Weitere Informationen finden Sie unter *Wiederherstellungsdatenträger erstellen und verwenden* (auf Seite 210).
2. Verwenden Sie ein anderes System, um das Laufwerk zu entschlüsseln. Weitere Informationen finden Sie unter *Mit PGP Whole Disk Encryption verschlüsselte Laufwerke entschlüsseln* (auf Seite 212).
3. Verwenden Sie das Whole Disk-Wiederherstellungs-Token. Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, wird das Wiederherstellungs-Token bei der Verschlüsselung des Laufwerks automatisch erstellt. Weitere Informationen finden Sie unter *Wiederherstellungs-Token verwenden* (auf Seite 209).

Wiederherstellungsdatenträger erstellen und verwenden

Obwohl die Wahrscheinlichkeit äußerst gering ist, dass ein Hauptstartdatensatz auf einem mit PGP Whole Disk Encryption verschlüsselten Startlaufwerk bzw. einer Startpartition beschädigt wird, kann dies nicht ausgeschlossen werden. In diesem Fall kann das System möglicherweise nicht gestartet werden.

Um sicherzustellen, dass Sie auf eine solche (unwahrscheinliche) Eventualität vorbereitet sind, sollten Sie eine Wiederherstellungs-CD oder -diskette (oder beides) erstellen, **bevor** Sie ein Startlaufwerk oder eine Startpartition mit PGP Whole Disk Encryption verschlüsseln.

Achtung: Beachten Sie, dass Wiederherstellungsdatenträger nur mit der Version von PGP Desktop kompatibel sind, mit der sie erstellt wurden. Wenn Sie beispielsweise versuchen, mit einem in Version 9.0.x erstellten Wiederherstellungsdatenträger ein mit PGP Whole Disk Encryption 9.5 geschütztes Laufwerk zu entschlüsseln, kann nicht mehr auf das PGP Whole Disk Encryption 9.5-Laufwerk zugegriffen werden.

Dieser Abschnitt enthält Verfahren zum Erstellen einer Wiederherstellungs-CD und einer Wiederherstellungsdiskette. Zudem wird die Verwendung erläutert.

▸ **So erstellen Sie eine Wiederherstellungs-CD:**

1. Vergewissern Sie sich, dass PGP Desktop für Windows sowie Roxio Easy Media Creator oder Roxio Easy CD Creator (bzw. eine andere Software, mit der eine CD von einem ISO-Image erstellt werden kann) auf dem System installiert sind.
2. Öffnen Sie Roxio Easy Media Creator bzw. Roxio Easy CD Creator und wählen Sie die Option zum Erstellen eines Daten-CD-Projekts.
3. Wählen Sie im Menü **Datei** die Option zum Aufzeichnen einer CD von einem CD-Image aus. Der Bildschirm zum Aufzeichnen einer CD vom Festplatten-Image wird angezeigt.
4. Wählen Sie als Dateityp **die Option für ISO-Bilddateien.**
5. Wechseln Sie zum PGP-Verzeichnis. Das Standardverzeichnis lautet `C:\Programme\PGP Corporation\PGP Desktop\`.
6. Wählen Sie `bootg.iso` aus und klicken Sie auf **Öffnen**. Der Einrichtungsbildschirm zum Aufzeichnen der CD wird angezeigt.
7. Legen Sie eine leere, beschreibbare CD in das CD-Laufwerk ein.
8. Klicken Sie im Einrichtungsbildschirm zum Aufzeichnen der CD auf die Option zum **Starten der Aufzeichnung. Der Bildschirm für den Fortschritt der Aufzeichnung der CD vom CD-Image wird angezeigt, während die ISO-Datei auf die CD geschrieben wird.**

9 Wenn die Datei auf die CD geschrieben wurde, klicken Sie auf **OK**. Die Wiederherstellungs-CD für PGP Whole Disk Encryption ist fertig.

10 Nehmen Sie die Wiederherstellungs-CD aus dem Laufwerk und beschriften Sie sie entsprechend.

So erstellen Sie eine Wiederherstellungsdiskette

1 Stellen Sie sicher, dass PGP Desktop für Windows sowie eine Anwendung, mit der eine Wiederherstellungsdiskette erstellt werden kann (z. B. MagicISO), auf dem System installiert sind.

2 Legen Sie eine leere Diskette in das Diskettenlaufwerk ein.

3 Öffnen Sie MagicISO.

4 Wählen Sie im Menü **Extras** die Option zum Schreiben des Disketten-Image. Das Dialogfeld „Öffnen“ wird angezeigt.

5 Wechseln Sie zum PGP-Verzeichnis. Das Standardverzeichnis lautet `C:\Programme\PGP Corporation\PGP Desktop\`.

6 Wählen Sie `Bootg.img` aus und klicken Sie auf **Öffnen**. Die Datei wird auf die Diskette geschrieben.

7 Nehmen Sie die Wiederherstellungsdiskette aus dem Laufwerk und beschriften Sie sie entsprechend.

8 Beenden Sie MagicISO.

So verwenden Sie eine Wiederherstellungs-CD oder -diskette

Achtung: Wenn Sie mit der Entschlüsselung eines Laufwerks oder einer Partition mit einer Wiederherstellungs-CD oder -diskette begonnen haben, halten Sie den Vorgang nicht an. Abhängig von der Größe des zu entschlüsselnden Laufwerks kann dieser Vorgang einige Zeit dauern. Sie können das Laufwerk schneller entschlüsseln, indem Sie ein anderes System verwenden, auf dem dieselbe Version von PGP Desktop installiert ist. Weitere Informationen finden Sie unter *Mit PGP Whole Disk Encryption verschlüsselte Laufwerke entschlüsseln* (auf Seite 212).

1 Wenn der Anmeldebildschirm von PGP Whole Disk Encryption beim Neustart des Systems nicht angezeigt wird oder wenn Sie beim Neustart zum Einlegen eines Wiederherstellungsdatenträgers für PGP Whole Disk Encryption aufgefordert werden, legen Sie die Wiederherstellungs-CD in das CD-Laufwerk bzw. die Wiederherstellungsdiskette in das Diskettenlaufwerk ein.

2 Starten Sie das System neu. Der Anmeldebildschirm für PGP Whole Disk Encryption vom Wiederherstellungsdatenträger wird angezeigt.

3 Geben Sie die entsprechende Passphrase für das mit PGP Whole Disk Encryption verschlüsselte Startlaufwerk bzw. die Startpartition ein. Sie haben folgende Möglichkeiten:

- Drücken Sie die **Eingabetaste**, um zu versuchen, das System zu starten.
- Geben Sie D ein, um das Laufwerk zu entschlüsseln.

Mit PGP Whole Disk Encryption verschlüsselte Laufwerke entschlüsseln

Wenn Sie auf einem Laufwerk, das mit PGP Whole Disk Encryption geschützt ist, Aktivitäten zur Laufwerkswiederherstellung durchführen müssen, empfiehlt die PGP Corporation die vorherige Entschlüsselung des Laufwerks. Sie haben folgende Möglichkeiten zum Entschlüsseln eines Laufwerks:

- Verwenden Sie in PGP Desktop die Option **Laufwerk > Entschlüsseln** (weitere Informationen zum Verwenden dieser Option zum Entschlüsseln eines Laufwerks finden Sie im folgenden Verfahren).
- Verwenden Sie den Wiederherstellungsdatenträger, den Sie für PGP Whole Disk Encryption vorbereitet haben (weitere Informationen zum Erstellen eines Wiederherstellungsdatenträgers finden Sie unter *Wiederherstellungsdatenträger erstellen* (siehe "Wiederherstellungsdatenträger erstellen und verwenden" auf Seite 210)).
- Schließen Sie die Festplatte über ein USB-Kabel an ein zweites System an und führen Sie die Entschlüsselung über PGP Desktop auf diesem System durch.

Wenn das Laufwerk entschlüsselt ist, können Sie mit der Wiederherstellung fortfahren.

So entschlüsseln Sie ein Laufwerk mit PGP Desktop

1 Öffnen Sie PGP Desktop und klicken Sie auf das Bedienfeld für PGP Disk. Das Bedienfeld für PGP Disk wird hervorgehoben.

2 Klicken Sie auf **Gesamte Festplatte oder Partition verschlüsseln**. Der Arbeitsbereich für das Verschlüssen der gesamten Festplatte (Partition) wird angezeigt und in einer Liste sind die Laufwerke des Systems aufgeführt, die mit PGP Whole Disk Encryption geschützt werden können: Laufwerke, Laufwerkspartitionen, Wechseldatenträger usw.

3 Klicken Sie oben im Arbeitsbereich **Gesamte Festplatte oder Partition verschlüsseln** im Bereich **Laufwerk oder Partition für Verschlüsselung auswählen** auf das Laufwerk oder die Partition, die Sie mit PGP Whole Disk Encryption entschlüsseln möchten.

4 Wählen Sie **Laufwerk** > **Entschlüsseln** oder klicken Sie auf **Entschlüsseln**. Das Dialogfeld „Laufwerk entsperren“ wird angezeigt.

5 Geben Sie die Passphrase zum Entsperren des Laufwerks ein. Im Fenster von PGP Desktop wird eine Fortschrittsanzeige für die Entschlüsselung angezeigt.

Auch die voraussichtliche Dauer zum Entschlüsseln des Laufwerks wird im Fenster von PGP Desktop angezeigt. Wenn Sie den Entschlüsselungsvorgang unterbrechen oder abbrechen möchten, klicken Sie auf **Anhalten**. Bei Bedarf können Sie den Computer herunterfahren, indem Sie **Start** > **Herunterfahren** auswählen. *Schalten Sie das System nicht über die Einschalttaste ab.*

So entschlüsseln Sie ein mit PGP Whole Disk Encryption verschlüsseltes Laufwerk mit einem anderen System

1 Entfernen Sie das Laufwerk, das Sie entschlüsseln möchten, aus dem Computer und legen Sie es in ein Laufwerksgehäuse.

2 Verbinden Sie das Laufwerksgehäuse über ein USB-Kabel mit einem Computer, auf dem PGP Desktop installiert ist.

3 Geben Sie auf dem Computer, auf dem PGP Desktop installiert ist, bei der Eingabeaufforderung die Passphrase ein, um das Laufwerk zu entschlüsseln, das sich im Laufwerksgehäuse befindet.

Spezielle Sicherheitsmaßnahmen von PGP Desktop

PGP Desktop verfügt über Funktionen, mit denen Sicherheitsprobleme mit PGP Whole Disk Encryption vermieden werden können. Diese Vorsichtsmaßnahmen gelten auch für PGP Virtual Disk-Laufwerke.

Löschung der Passphrase

Wenn Sie eine Passphrase eingeben, wird diese von PGP Desktop nur für kurze Zeit verwendet und danach aus dem Speicher gelöscht. PGP Desktop erstellt außerdem keine Kopien der Passphrase. Daher befindet sich die Passphrase in der Regel nur für den Bruchteil einer Sekunde im Speicher. Diese Funktion ist von größter Bedeutung, da sonst andere Personen im Hauptspeicher nach der Passphrase suchen könnten, während Sie nicht an Ihrem Arbeitsplatz sind. Diese Personen würden dann ohne Ihr Wissen vollständigen Zugriff auf alle mit dieser Passphrase geschützten Daten erhalten.

Schutz des virtuellen Speichers

Ihre Passphrase oder andere Schlüssel könnten mit den Daten des virtuellen Speichersystems auf die Festplatte ausgelagert werden. PGP Desktop lässt jedoch nicht zu, dass die Passphrasen und Schlüssel auf die Festplatte geschrieben werden. Mit dieser Funktion wird verhindert, dass unberechtigte Personen die virtuelle Speicherdatei nach Passphrasen durchsuchen.

Ruhezustand und Standbymodus

In Windows wird beim Ruhezustand ein Image des gesamten Hauptspeichers des Computers in eine Datei auf der Festplatte geschrieben. Dies umfasst jedoch *nicht* Ihre Passphrase. Die PGP Corporation empfiehlt, dass Sie immer den Ruhezustand und nicht die Standbyfunktion verwenden, da der Computer im Ruhezustand ausgeschaltet wird und Sie sich beim PGP BootGuard-Bildschirm zur Anmeldung erneut authentifizieren müssen.

Schutz durch MSIM (Memory Static Ion Migration)

Wenn Sie ein Laufwerk oder eine Partition (unter Windows) mit PGP Whole Disk Encryption schützen, wird Ihre Passphrase in einen Schlüssel umgewandelt. Dieser Schlüssel dient zum Verschlüsseln und Entschlüsseln der Daten auf dem verschlüsselten Laufwerk bzw. der verschlüsselten Partition. Obwohl die Passphrase sofort aus dem Speicher gelöscht wird, bleibt der Schlüssel (aus dem die Passphrase nicht abgeleitet werden kann) jedoch im Speicher erhalten.

Dieser Schlüssel wird zwar nicht im virtuellen Speicher gespeichert, wenn jedoch ein bestimmter Speicherbereich genau dieselben Daten für extrem lange Zeiträume speichert, ohne dass der Computer ausgeschaltet oder zurückgesetzt wird, bleibt eine statische Ladung im Speicher zurück, die von Angreifern gelesen werden könnte. Wenn Ihr verschlüsseltes Laufwerk bzw. Ihre verschlüsselte Partition (unter Windows) für einen langen Zeitraum entschlüsselt ist, können mit der Zeit erkennbare Spuren des Schlüssels im Speicher zurückbleiben. Mit bestimmten Geräten könnte der Schlüssel wiederhergestellt werden. Diese Geräte sind zwar nicht im Elektronikfachgeschäft um die Ecke zu finden, stehen wahrscheinlich jedoch größeren Regierungsbehörden zur Verfügung.

PGP Desktop schützt vor derartigen Angriffen, indem zwei Kopien (eine normale Kopie und eine Kopie mit umgekehrten Bit) im RAM-Speicher gehalten und alle paar Sekunden umgekehrt werden.

Weitere Sicherheitsaspekte

Im Allgemeinen hängt die Fähigkeit zum Schützen von Daten von den Vorkehrungen ab, die Sie treffen. Kein Verschlüsselungsprogramm kann Sie vor unzureichenden Sicherheitsmaßnahmen schützen. Wenn Sie sich z. B. vom Schreibtisch entfernen und dabei den Computer eingeschaltet und vertrauliche Dateien geöffnet lassen, kann jeder auf die Informationen zugreifen, auch wenn das Laufwerk oder die Partition (unter Windows) mit PGP Whole Disk Encryption geschützt ist.

Im Folgenden sind einige Empfehlungen zur Wahrung der optimalen Sicherheit aufgeführt:

- Verwenden Sie einen Bildschirmschoner mit Kennwortschutz, um anderen Personen den Zugriff auf Ihren Computer oder das Anzeigen Ihres Bildschirms zu erschweren, wenn Sie sich nicht an Ihrem Schreibtisch befinden.
- Stellen Sie sicher, dass die verschlüsselten Laufwerke oder Partitionen (unter Windows) nicht für andere Computer im Netzwerk freigegeben sind. Wenden Sie sich dazu ggf. an den Netzwerkadministrator. Wenn Sie Laufwerke oder Partitionen entsperrt haben, wird der Inhalt nicht mehr durch PGP Whole Disk Encryption geschützt. Sie können von allen Personen angezeigt werden, die im Netzwerk darauf zugreifen können. Verwenden Sie PGP Virtual Disk zum Speichern von Dateien, die auch gesperrt bleiben müssen, während Sie am Computer arbeiten.
- Schreiben Sie Ihre Passphrase auf keinen Fall auf. Wählen Sie eine Passphrase, die Sie sich merken können. Wenn Sie sich die Passphrase nur schwer merken können, verwenden Sie eine Gedächtnisstütze (z. B. Poster, Lieder, Gedichte oder Witze), jedoch *schreiben Sie die Passphrase nicht auf*.
- Wenn Sie PGP Desktop zu Hause einsetzen und den Computer gemeinsam mit anderen Personen nutzen, können diese wahrscheinlich Ihre geöffneten Dateien sehen, die sich auf mit PGP Whole Disk Encryption geschützten Laufwerken oder Partitionen (unter Windows) befinden. Solange Sie ein System mit durch PGP Whole Disk Encryption verschlüsselten Laufwerken oder Partitionen herunterfahren oder einen verschlüsselten Datenträger aus dem System entfernen, bleiben alle Dateien auf dem Laufwerk, der Partition bzw. dem Datenträger verschlüsselt und vollständig geschützt.

Windows-Vorinstallationsumgebung verwenden

Durch das Erstellen einer benutzerdefinierten Windows-CD/UFD-Vorinstallationsumgebung (USB-Flash-Laufwerk) erhalten Sie ein startfähiges Wiederherstellungstool, das in Notfällen verwendet werden kann. Sie können beispielsweise DOS-Befehle zum Kopieren, Bearbeiten, Sichern und Löschen von Dateien verwenden.

Darüber hinaus können Sie die Windows-Vorinstallationsumgebung verwenden, um ein Upgrade eines mit PGP WDE verschlüsselten Computers auf Windows Vista durchzuführen.

Informationen zum Erhalten der PGP WDE-Treiber und -Tools finden Sie im *Wissensdatenbankartikel 807* (https://support.pgp.com/?faq=807). Dieser Artikel enthält auch einen technischen Hinweis, den Sie herunterladen können und der alle Anleitungen in diesem Abschnitt enthält.

PGP Whole Disk Encryption mit IBM Lenovo ThinkPad-Systemen verwenden

Verwenden Sie die Windows-Vorinstallationsumgebung (PE), um den PGP WDE-Treiber in IBM Lenovo ThinkPad Rescue & Recovery vorzuinstallieren und die Lenovo Rescue & Recovery-Funktion automatisch zu erkennen.

Diese Option steht nur für IBM Lenovo-Systeme zur Verfügung, auf denen Version 3.0 oder höher von Rescue & Recovery ausgeführt wird. Durch diese Option wird der PGP WDE-Treiber in Lenovo Rescue & Recovery vorinstalliert und die Unterstützung für Lenovo Rescue & Recovery wird automatisch erkannt. Der PGP WDE-Treiber wird im Verzeichnis \windows\system32\drivers gesucht. In IBM Lenovo Rescue & Recovery werden zwei Dateien installiert: der PGP WDE-Treiber (`pgpwded.sys`) und die Datei `PGPstart.exe` (weitere Informationen zu dieser Datei finden Sie im folgenden Verfahren).

Folgende Dateien sind zur Installation von PGP Whole Disk Encryption in IBM Lenovo Rescue & Recovery erforderlich:

- Dateien vom pgppe-Tool: `pgppe.exe`, `pgpstart.exe`
- Dateien von der PGP Desktop-Installation: `pgpwded.sys`, `pgpbootb.bin`, `pgpbootg.bin`, `pgpsdk.dll`, `pgpsdknl.dll`, `pgpwd.dll`, `pgpwde.exe`
- Dateien ausschließlich für Windows Vista: wimfltr-Treiber müssen installiert werden (Teil des Windows Automated Installation Kit)

Achtung: Verwenden Sie diese Option erst, wenn PGP Desktop auf dem System installiert ist.

So aktivieren Sie Lenovo Rescue & Recovery

1. Installieren Sie PGP Desktop.
2. Installieren Sie die Tools für die Windows-Vorinstallationsumgebung, die über den *PGP-Wissensdatenbankartikel 807* (https://support.pgp.com/?faq=807) erhältlich sind.
3. Kopieren Sie die Dateien `PGPstart.exe` und `PGPpe.exe` aus der komprimierten Datei in das Installationsverzeichnis von PGP Desktop (standardmäßig `c:\Programme\PGP Corporation\PGP Desktop`).

4 Rufen Sie eine Eingabeaufforderung auf und wechseln Sie zum PGP Desktop-Verzeichnis.

5 Führen Sie den Befehl „pgppe“ wie folgt aus:

```
pgppe /recovery
```

So entfernen Sie die Unterstützung für Lenovo Rescue & Recovery

Führen Sie den Befehl „pgppe“ wie folgt aus: `pgppe /recovery /remove`

PGP Whole Disk Encryption mit der Microsoft Windows XP-Wiederherstellungskonsole verwenden

Wenn Sie die Windows XP-Wiederherstellungskonsole zu Administrationszwecken verwenden, müssen Sie die PGP WDE-Treiber für die Microsoft Windows-Wiederherstellungskonsole beim Verschlüsseln des Laufwerks installieren, da die Wiederherstellungskonsole andernfalls nicht verwendet werden kann.

Hinweis: Sie müssen Passphrasenbenutzer verwenden, wenn Benutzer mit Windows PE oder BartPE authentifiziert werden sollen. Token- oder TPM-Benutzer werden nicht unterstützt.

Achtung: Installieren Sie diese Treiber erst, nachdem PGP Desktop installiert und das Laufwerk mit PGP Whole Disk Encryption verschlüsselt wurde.

So installieren Sie die PGP WDE-Treiber für die Windows XP-Wiederherstellungskonsole

1 Installieren Sie PGP Desktop.

2 Installieren Sie die Tools für die Windows-Vorinstallationsumgebung, die über den *PGP-Wissensdatenbankartikel 807* (https://support.pgp.com/?faq=807) erhältlich sind.

3 Kopieren Sie die Dateien `PGPstart.exe` und `PGPpe.exe` aus der komprimierten Datei in das Installationsverzeichnis von PGP Desktop (standardmäßig `c:\Programme\PGP Corporation\PGP Desktop`).

4 Rufen Sie eine Eingabeaufforderung auf und wechseln Sie zum Installationsverzeichnis von PGP Desktop.

5 Führen Sie den Befehl „pgppe“ wie folgt aus:

```
pgppe /cmdcons
```

So entfernen Sie Treiber aus der Windows XP-Wiederherstellungskonsole

Führen Sie den Befehl „pgppe“ wie folgt aus: `pgppe /cmdcons /remove`

11 PGP Virtual Disk-Laufwerke verwenden

Sie können mit PGP Virtual Disk-Laufwerken Ihre Dateien organisieren, Dateien mit ähnlichen Namen getrennt speichern oder mehrere Versionen derselben Dokumente und Programme separat verwalten.

In diesem Abschnitt wird die PGP Virtual Disk-Funktion von PGP Desktop beschrieben.

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung verwenden, hat Ihr PGP Universal Server-Administrator ggf. bestimmte Funktionen deaktiviert. Ist eine Funktion deaktiviert, wird das Bedienelement auf der linken Seite nicht angezeigt und das Menü oder andere auf diese Funktion zutreffenden Optionen sind nicht verfügbar. Die in diesem Handbuch enthaltenen Abbildungen entsprechen der Standardinstallation, bei der alle Funktionen aktiviert sind. Wenn Ihr PGP Universal Server-Administrator diese Funktion deaktiviert hat, ist dieser Abschnitt für Sie nicht relevant.

In diesem Kapitel

Informationen zu PGP Virtual Disk-Laufwerken 220
Neue PGP Virtual Disk-Laufwerke erstellen 221
Eigenschaften von PGP Virtual Disk-Laufwerken anzeigen 225
PGP Virtual Disk-Laufwerke suchen 225
Aktivierte PGP Virtual Disk-Laufwerke verwenden 226
Mit anderen Benutzern arbeiten 230
Benutzer-Passphrasen ändern 233
PGP Virtual Disk-Laufwerke löschen 234
PGP Virtual Disk-Laufwerke warten 235
PGP Virtual Disk-Verschlüsselungsalgorithmen 237
Spezielle Sicherheitsfunktionen von PGP Virtual Disk 237

Hinweis: In früheren Versionen von PGP Desktop wurden PGP Virtual Disk-Laufwerke als *PGP Disk*-Laufwerke bezeichnet. Die Bezeichnung *PGP Disk* umfasst jetzt sowohl die Funktionen PGP Virtual Disk als auch PGP Whole Disk Encryption.

Informationen zu PGP Virtual Disk-Laufwerken

Ein PGP Virtual Disk-Laufwerk ist ein Speicherplatzbereich auf einem mit dem Computer verbundenen Datenträger. Dieser Speicherplatzbereich wird verschlüsselt und separat verwaltet. PGP Virtual Disk-Laufwerke sind mit einem Banktresor vergleichbar und eignen sich hervorragend für den Schutz vertraulicher Dateien, während der Rest des Computers unverschlüsselt zur Verfügung steht.

Die Funktionsweise eines PGP Virtual Disk-Laufwerks ist mit der eines zusätzlichen Festplattenlaufwerks zu vergleichen, obwohl es sich eigentlich um eine einzelne Datei handelt, die sich auf einer beliebigen Festplatte des Computers befinden kann. Die Datei bietet Speicherplatz für Dateien jeden Typs. Auf einem PGP Virtual Disk-Laufwerk können Sie sogar Anwendungen installieren oder Dateien speichern. Das Besondere daran ist jedoch, dass sich ein solches Laufwerk jederzeit und ohne Auswirkungen auf den Rest des Computers sperren lässt. Wenn Sie die auf einem PGP Virtual Disk-Laufwerk gespeicherten Anwendungen oder Dateien verwenden möchten, entsperren Sie das Laufwerk. Dadurch können Sie wieder auf die Dateien zugreifen.

PGP Virtual Disk-Laufwerke werden entsperrt und gesperrt, indem sie auf dem Computer aktiviert bzw. deaktiviert werden. PGP Desktop unterstützt Sie bei diesem Vorgang.

Die Größe eines PGP Virtual Disk-Laufwerks kann festgelegt werden, jedoch ist auch die Erstellung eines dynamisch dimensionierten Laufwerks möglich, dessen Kapazität bei Bedarf erweitert wird. Die Größe, die Sie bei der Erstellung des Laufwerks vorgeben, bezeichnet die maximale Größe des Laufwerks.

Nach der Aktivierung eines PGP Virtual Disk-Laufwerks sind folgende Aktionen möglich:

- Verschieben oder Kopieren von Dateien auf das aktivierte PGP Virtual Disk-Laufwerk bzw. von diesem Laufwerk
- Speichern von Dateien auf dem aktivierten PGP Virtual Disk-Laufwerk
- Installieren von Anwendungen auf dem PGP Virtual Disk-Laufwerk

Dateien und Anwendungen auf einem PGP Virtual Disk-Laufwerk werden verschlüsselt gespeichert. Falls der Computer während der Deaktivierung eines PGP Virtual Disk-Laufwerks abstürzt, bleibt der Inhalt des Laufwerks sicher verschlüsselt.

Deaktivierte PGP Virtual Disk-Laufwerke werden nicht in Windows Explorer oder im Finder von Mac OS X aufgeführt und sind für Benutzer ohne korrekte Authentifizierung nicht zugänglich.

Beachten Sie, dass die Daten in der verschlüsselten Datei sicher gespeichert bleiben und nur entschlüsselt werden, wenn Sie auf eine der Dateien zugreifen. Durch diese Art der Datenspeicherung können PGP Virtual Disk-Laufwerke problemlos bearbeitet und mit anderen Personen ausgetauscht werden, jedoch gehen die Daten verloren, wenn die Laufwerksdatei gelöscht wird. Es ist daher ratsam, Sicherungskopien der verschlüsselten Dateien zu erstellen, damit die Daten im Notfall wiederhergestellt werden können.

Informationen zu PGP-Optionen für PGP Virtual Disk-Laufwerke finden Sie unter *Laufwerksoptionen* (auf Seite 342).

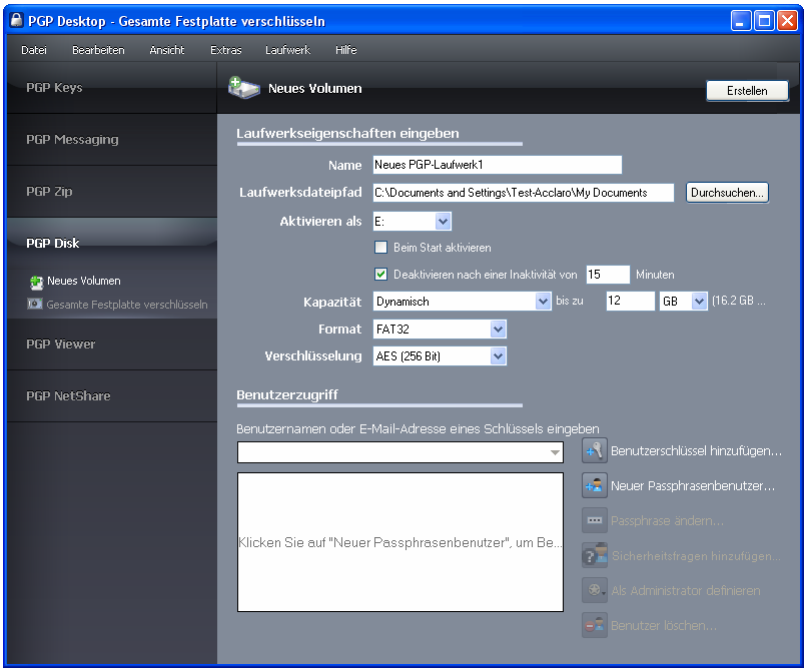
Achtung: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, müssen Sie nach der Installation von PGP Desktop möglicherweise ein PGP Virtual Disk-Laufwerk erstellen. In diesem Fall wurden Größe, Dateisystem und Algorithmus u. U. festgelegt. Weitere Informationen finden Sie unter *PGP Desktop mit PGP Universal Server verwenden* (auf Seite 357).

Neue PGP Virtual Disk-Laufwerke erstellen

So erstellen Sie ein neues PGP Virtual Disk-Laufwerk

1 Öffnen Sie PGP Desktop.

2 Klicken Sie im linken Fensterbereich des Hauptbildschirms von PGP Desktop auf das Bedienfeld „PGP Disk“ und klicken Sie auf **Neues Volumen. Sie können auch auf Datei > Neu > PGP Virtual Disk** klicken. Der Bildschirm „Neues Volumen“ wird im rechten Bildschirmbereich angezeigt.



3 Geben Sie in das Feld **Name** einen Namen für das neue PGP Virtual Disk-Laufwerk ein.

4 Übernehmen Sie den Standardspeicherort für das neue PGP Virtual Disk-Laufwerk, der im Feld **Laufwerksdateipfad** angezeigt wird, oder klicken Sie auf **Durchsuchen** und geben Sie einen anderen Speicherort an.

5 Wählen Sie im Menü **Aktivieren als** den Laufwerksbuchstaben aus, der dem neuen PGP Virtual Disk-Laufwerk zugewiesen werden soll.

Sie haben folgende Möglichkeiten:

- Übernehmen Sie den Laufwerksbuchstaben, der von PGP Desktop vorgeschlagen wird.
- Wählen Sie im Menü **Aktivieren als** einen verfügbaren Laufwerksbuchstaben aus der Liste aus.
- Wählen Sie im Menü **Aktivieren als** die Option **Ordner** aus, wenn Sie das neue PGP Virtual Disk-Laufwerk einem Ordner anstelle eines Laufwerksbuchstabens zuweisen möchten. In diesem Fall wird neben dem Menü **Aktivieren als** ein Feld angezeigt, in dem Sie den Speicherort des Ordners angeben können.

6 Wählen Sie **Beim Start aktivieren** aus, wenn das neue PGP Virtual Disk-Laufwerk beim Starten automatisch aktiviert werden soll. Wenn diese Option aktiviert ist, werden Sie beim Systemstart zur Eingabe der Passphrase für das PGP Virtual Disk-Laufwerk aufgefordert.

7 Mit der Option **Deaktivieren nach einer Inaktivität von n Minuten** (*n* steht für die Anzahl der Minuten) können Sie eine automatische Deaktivierung des PGP Virtual Disk-Laufwerks veranlassen, wenn der Computer eine bestimmte Zeitspanne (in Minuten) nicht verwendet wird. Verwenden Sie diese Option, wenn Sie den Computer häufig unbeaufsichtigt lassen. Durch diese zusätzliche Sicherheitsmaßnahme wird das PGP Virtual Disk-Laufwerk automatisch gesperrt, wenn Sie vergessen, es zu deaktivieren.

8 Wählen Sie im Menü **Kapazität** den gewünschten Typ für das PGP Virtual Disk-Laufwerk aus. Folgende Optionen sind verfügbar:

- **Dynamisch (anpassbare Größe)**: Die Kapazität dieses Laufwerkstyps erhöht sich automatisch, wenn neue Dateien hinzugefügt werden. Solange der zusätzliche Speicherplatz nicht benötigt wird, bleibt die Größe des Laufwerks klein. Dieser Vorgang wird von PGP Desktop automatisch verwaltet. Sie müssen lediglich die Maximalgröße des Laufwerks festlegen. Auf Wunsch können Sie dieses Laufwerk später auch komprimieren. Diese Art des PGP Virtual Disk-Laufwerks ist nur für Laufwerke im FAT- oder FAT32-Format verfügbar.
- **Erweiterbar**: Die Kapazität dieses Laufwerkstyps erhöht sich automatisch, wenn neue Dateien hinzugefügt werden. Solange der zusätzliche Speicherplatz nicht benötigt wird, bleibt die Größe des Laufwerks klein. Dieser Vorgang wird von PGP Desktop automatisch verwaltet. Sie müssen lediglich die Maximalgröße des Laufwerks festlegen. Auf Wunsch können Sie dieses Laufwerk später auch komprimieren. Diese Art des PGP Virtual Disk-Laufwerks ist nur für Laufwerke im NTFS-Format verfügbar.
- **Feste Größe**: Dieser Laufwerkstyp hat unabhängig von der Anzahl der hinzugefügten Dateien immer dieselbe Kapazität. Diese Art des PGP Virtual Disk-Laufwerks ist für Laufwerke in jedem beliebigen Format verfügbar.

9 Legen Sie über das Menü **Kapazität** die Größe des neuen PGP Virtual Disk-Laufwerks fest (geben Sie für dynamische Laufwerke die maximale Größe an). Geben Sie ganze Zahlen ohne Dezimalstellen ein. Wählen Sie im Menü die Option **KB** (Kilobyte), **MB** (Megabyte) oder **GB** (Gigabyte) aus.

Die maximal zulässige Größe für ein PGP Virtual Disk-Laufwerk hängt von der Größe und dem Format der Festplatte ab.

10 Geben Sie ein Dateisystemformat für das Laufwerk an:

- **FAT**: Das Laufwerk muss mindestens 100 KB groß sein.
- **FAT32**: Das Laufwerk muss mindestens 260 MB groß sein.
- **NTFS**: Das Laufwerk muss mindestens 5 MB groß sein (12 MB für Windows Vista).

11 Legen Sie den Verschlüsselungsalgorithmus fest, den Sie zum Schutz der Daten verwenden möchten:

- **AES (256 Bit)**: AES (Advanced Encryption Standard) ist ein Block-Algorithmus, der bei 128, 192 oder 256 Bit verwendet werden kann. Standardmäßig wird die sicherere 256-Bit-Version zum Erstellen von PGP Virtual Disk-Laufwerken verwendet.
- **EME2-AES (256 Bit)**: EME2 (Encrypt-Mix-Encrypt v2) ist ein stärkerer Algorithmus, der jeden Vorgang doppelt verschlüsselt. EME2 ist ein Wide-Block-Algorithmus, der derzeit von der Arbeitsgruppe für IEEE-Standards geprüft wird.
- **CAST5 (128 Bit)**: CAST ist ein 128-Bit-Block-Algorithmus. CAST ist ein starker Verschlüsselungsalgorithmus für die militärische Verwendung, der als undurchdringbar für unbefugten Zugriff gilt.
- **Twofish (256 Bit)**: Twofish ist ein symmetrischer 256-Bit-Block-Algorithmus. Er gehörte zu den fünf Algorithmen, die das US-amerikanische National Institute of Standards and Technology (NIST) für den erweiterten Verschlüsselungsstandard (AES) in Betracht gezogen hatte (ausgewählt wurde Rijndael).

12 Mindestens ein Benutzer muss auf das neue PGP Virtual Disk-Laufwerk zugreifen können. Geben Sie im Bereich **Benutzerzugriff** die Personen an, denen Sie Zugriff gewähren möchten, und legen Sie die Zugriffsmethode fest:

- **Benutzerschlüssel**: Fügen Sie Benutzer, die sich mit Kryptographie mit öffentlichem Schlüssel authentifizieren, folgendermaßen hinzu:
  - Klicken Sie auf **Benutzerschlüssel hinzufügen**. Das Feld „Schlüsselbenutzer hinzufügen“ wird mit den derzeit am Schlüsselbund befindlichen Schlüsselpaaren angezeigt.
  - Wählen Sie im Feld **Schlüsselbenutzer hinzufügen** die gewünschten Schlüsselbenutzer aus, indem Sie auf den betreffenden Listeneintrag doppelklicken. Sie können stattdessen auch den Listeneintrag von der linken Seite nach rechts ziehen oder einen Listeneintrag auswählen und auf **Hinzufügen** klicken. Klicken Sie abschließend auf **OK**.
- **Passphrase**: Klicken Sie auf **Neuer Passphrasenbenutzer**. Das Dialogfeld „Neuen Benutzer erstellen“ wird angezeigt.
  - Geben Sie für jeden neuen Passphrasenbenutzer einen Namen und eine Passphrase für den Benutzer ein. Geben Sie die Passphrase zur Bestätigung erneut ein. Klicken Sie auf **OK**, um den Passphrasenbenutzer zu erstellen. Wiederholen Sie ggf. den Vorgang, wenn Sie weitere Passphrasenbenutzer autorisieren möchten.
  - Wenn Sie die Passphrase eines Passphrasenbenutzers ändern möchten, wählen Sie den Benutzer aus und klicken Sie auf **Passphrase ändern**.

Informationen zum Erstellen von effektiven, hochwertigen Passphrasen finden Sie unter *Starke Passphrasen erstellen* (auf Seite 353).

13 Klicken Sie auf **Erstellen**, um die Erstellung des neuen PGP Virtual Disk-Laufwerks zu starten. In einer Fortschrittsanzeige wird angezeigt, welcher Anteil des PGP Virtual Disk-Laufwerks bereits initialisiert und formatiert ist. Nach Abschluss des Vorgangs wird das neue PGP Virtual Disk-Laufwerk im Bedienfeld „PGP Disk“ angezeigt.

14 Der erste Benutzer, den Sie erstellen, erhält den Status eines Administrators. Es kann jeweils immer nur einen Administrator geben. Sie können jedoch einem beliebigen anderen Benutzer den Administratorstatus zuweisen, unabhängig davon, ob es sich um einen Benutzer öffentlicher Schlüssel oder um einen Passphrasenbenutzer handelt. Klicken Sie in der Liste „Benutzerzugriff“ auf den Namen der gewünschten Person und klicken Sie dann auf **Als Administrator definieren**.

15 Löschen Sie einen Benutzer (mit Ausnahme des Administrators), indem Sie den entsprechenden Namen auswählen und auf **Benutzer löschen** klicken. Der Administrator kann erst gelöscht werden, nachdem ein anderer Benutzer als Administrator definiert wurde.

Eigenschaften von PGP Virtual Disk-Laufwerken anzeigen

Nachdem Sie ein PGP Virtual Disk-Laufwerk erstellt haben, können Sie im Bildschirm „Laufwerkseigenschaften“ auf Informationen zum Laufwerk sowie zu den Einstellungen zugreifen, die geändert werden können.

So zeigen Sie die Eigenschaften eines PGP Disk-Laufwerks an

- Klicken Sie im linken Fensterbereich des Hauptbildschirms von PGP Desktop auf das Bedienfeld PGP Disk, und klicken Sie anschließend auf den Namen des Laufwerks. Die Laufwerkseigenschaften werden rechts im Hauptbildschirm angezeigt. Zu den angezeigten Informationen gehören PGP Virtual Disk-Dateipfad, Laufwerkskapazität, aktivierter Laufwerksbuchstabe, Laufwerksformat, Verschlüsselungstyp und Status des Laufwerks (aktiviert oder deaktiviert).

PGP Virtual Disk-Laufwerke suchen

Wenn Sie bereits mit früheren Installationen von PGP Desktop ein oder mehrere PGP Virtual Disk-Laufwerke erstellt haben, können Sie diese mit dem Suchassistenten für PGP-Laufwerke problemlos finden.

So suchen Sie PGP Virtual Disk-Laufwerke auf dem System

1. Klicken Sie in PGP Desktop auf das Bedienfeld **PGP Disk**. Der Hauptbildschirm von PGP Disk wird angezeigt.
2. Wählen Sie **Datei > Durchsuchen nach PGP-Laufwerken**. Daraufhin wird der Suchassistent für PGP-Laufwerke angezeigt.
3. Folgen Sie den im Assistenten angezeigten Anweisungen.

Tipp: Wenn Sie das aktivierte Laufwerk eines bestimmten PGP Virtual Disk-Laufwerks suchen möchten, klicken Sie in PGP Desktop mit der rechten Maustaste auf den Namen des Laufwerks und wählen Sie **Laufwerksspeicherort in Explorer anzeigen** aus. Windows Explorer öffnet ein neues Fenster, in dem der Inhalt des Laufwerks angezeigt wird.

Aktivierte PGP Virtual Disk-Laufwerke verwenden

Sie können Dateien und Ordner auf einem PGP Virtual Disk-Laufwerk wie auf jedem anderen Laufwerk des Systems erstellen, kopieren, verschieben und löschen.

Andere Personen mit Zugriff auf das Laufwerk (entweder auf demselben Computer oder über ein Netzwerk) können ebenfalls auf die darauf gespeicherten Daten zugreifen. Die Daten werden erst geschützt, wenn Sie das Laufwerk deaktivieren.

Achtung: Obwohl die PGP Virtual Disk-Laufwerksdatei verschlüsselt und vor unbefugtem Zugriff geschützt ist, kann sie dennoch von der Festplatte gelöscht werden. Alle Personen mit Zugriff auf Ihr System könnten die verschlüsselte Datei mit dem PGP Virtual Disk-Laufwerk löschen. Daher sollten Sie eine Sicherungskopie der verschlüsselten Datei aufbewahren und den Computer sperren, wenn Sie nicht in der Nähe sind.

PGP Virtual Disk-Laufwerke aktivieren

Wenn Sie ein neues PGP Virtual Disk-Laufwerk erstellen, wird es automatisch aktiviert, sodass Sie es sofort zum Speichern von Dateien einsetzen können.

Damit Sie den Inhalt eines Laufwerks sichern können, müssen Sie es deaktivieren. Nach dem Deaktivieren des Laufwerks sind die Daten sicher in einer verschlüsselten Datei gespeichert und der Zugriff ist erst möglich, wenn das Laufwerk wieder aktiviert wird.

Es gibt verschiedene Möglichkeiten, ein PGP Virtual Disk-Laufwerk zu aktivieren:

- Wählen Sie in PGP Desktop das PGP Virtual Disk-Laufwerk aus, das Sie aktivieren möchten, und wählen Sie **Laufwerk > Aktivieren** aus.

- Wählen Sie in PGP Desktop das PGP Virtual Disk-Laufwerk aus, das Sie aktivieren möchten, und klicken Sie unter Windows in der oberen rechten Ecke auf **Aktivieren** oder unter Mac OS X in der Symbolleiste auf das Symbol **Aktivieren**.
- Ändern Sie die Eigenschaften des PGP Virtual Disk-Laufwerks, sodass es beim Start des Computers aktiviert wird.

Nur unter Windows:

- Aktivieren Sie während der Erstellung des PGP Virtual Disk-Laufwerks das Kontrollkästchen **Beim Start aktivieren**. Das Laufwerk wird dann beim Start von Windows automatisch aktiviert. Wenn Sie diese Option nicht beim Erstellen des PGP Virtual Disk-Laufwerks aktivieren, können Sie dies später nachholen.
- Klicken Sie in Windows Explorer mit der rechten Maustaste auf die PGP Virtual Disk-Datei und wählen Sie im Kontextmenü die Option **PGP > PGP Virtual Disk-Laufwerk aktivieren** aus.

Aktivierte PGP Virtual Disk-Laufwerke werden in Windows Explorer und im Finder von Mac OS X als leere Laufwerke angezeigt.

PGP Virtual Disk-Laufwerke deaktivieren

Sie können ein PGP Virtual Disk-Laufwerk sperren, indem Sie es deaktivieren. Nach dem Deaktivieren eines PGP Virtual Disk-Laufwerks ist dessen Inhalt in der verschlüsselten Laufwerksdatei gesperrt. Der Inhalt ist erst dann wieder zugänglich, wenn das Laufwerk wieder aktiviert wird.

Achtung: Wenn Sie ein PGP Virtual Disk-Laufwerk deaktivieren und darauf gespeicherte Dateien geöffnet sind, können Daten verloren gehen. Geben Sie Optionen für die Deaktivierung von Laufwerken an, indem Sie **Extras > PGP** auswählen und auf die Registerkarte **Laufwerk** klicken. Eine Option lautet **Deaktivierung von PGP-Laufwerken zulassen, wenn Dateien geöffnet sind**. Wenn diese Option ausgewählt ist, ist auch die Option **Keine Bestätigung zum Deaktivieren anfordern** verfügbar. **Verwenden Sie diese Optionen nur, wenn Sie damit vertraut sind.** Diese Optionen sind zwar für fortgeschrittene Benutzer hilfreich, die Ihre Daten regelmäßig sichern, sind jedoch für die meisten Benutzer nicht zu empfehlen.

Es gibt verschiedene Möglichkeiten, ein PGP Virtual Disk-Laufwerk zu deaktivieren:

- Klicken Sie im linken Fensterbereich des Hauptbildschirms von PGP Desktop auf das Bedienfeld „PGP Disk“ und wählen Sie das Laufwerk aus, das Sie deaktivieren möchten. Klicken Sie oben rechts auf **Deaktivieren** oder wählen Sie **Laufwerk > Deaktivieren aus.**
- Klicken Sie in Windows Explorer mit der rechten Maustaste auf die Datei des PGP Virtual Disk-Laufwerks und wählen Sie im Kontextmenü die Option **PGP > PGP Virtual Disk deaktivieren** aus.

- Verwenden Sie den Tastaturbefehl, um alle PGP Virtual Disk-Laufwerke zu deaktivieren. Der Standard-Tastaturbefehl ist **Strg+Umschalt+U**. Der Tastaturbefehl muss zuerst aktiviert werden.

Nach dem Deaktivieren eines PGP Virtual Disk-Laufwerks bleiben die Daten gesperrt und der Zugriff ist erst möglich, wenn das Laufwerk wieder aktiviert wird.

PGP Virtual Disk-Laufwerke komprimieren

Sie können zusätzlichen Speicherplatz auf dem PGP Virtual Disk-Laufwerk freigeben, indem Sie das Laufwerk komprimieren. Wenn das PGP Virtual Disk-Laufwerk aktiviert ist, müssen Sie das Laufwerk zunächst deaktivieren, bevor es komprimiert werden kann.

Hinweis: Nur PGP Virtual Disk-Laufwerke im FAT- oder FAT32-Format, die dynamisch sind (keine feste Größe), können komprimiert werden. Laufwerke im NTFS-Format oder Laufwerke mit fester Größe können nicht komprimiert werden.

So komprimieren Sie ein PGP Virtual Disk-Laufwerk

- Führen Sie einen der folgenden Schritte aus:
  - Wechseln Sie in Windows Explorer zum Speicherort der PGD-Datei. Klicken Sie mit der rechten Maustaste auf die Datei und wählen Sie **PGP Desktop > Nicht verwendeten Speicherplatz komprimieren** aus.
  - Klicken Sie in PGP Desktop im linken Bereich des Hauptbildschirms von PGP Desktop auf das Bedienfeld „PGP Disk“, wählen Sie das PGP Virtual Disk-Laufwerk aus, das Sie komprimieren möchten, und klicken Sie anschließend auf **Laufwerk > Komprimieren**. Sie können auch mit der rechten Maustaste im Bedienfeld „PGP Disk“ auf das PGP Virtual Disk-Laufwerk klicken und im Kontextmenü die Option **Komprimieren** auswählen.

PGP Virtual Disk-Laufwerke umschlüsseln

Sie können die auf einem PGP Virtual Disk-Laufwerk gespeicherten Daten umschlüsseln. Dies kann aus einem von zwei (oder beiden) Gründen erfolgen:

- Sie möchten den Verschlüsselungsalgorithmus ändern, mit dem das Laufwerk derzeit geschützt ist.
- Sie vermuten, dass ein Sicherheitsverstoß aufgetreten ist.

Bei der Umschlüsselung wird das PGP Virtual Disk-Laufwerk erneut verschlüsselt, jedoch wird ein anderer zugrunde liegender Verschlüsselungsschlüssel verwendet.

Achtung: Erfahrene Benutzer können in der Lage sein, den Speicher eines Computers nach dem zugrunde liegenden Verschlüsselungsschlüssel eines PGP Virtual Disk-Laufwerks zu durchsuchen. Diese Benutzer könnten den Schlüssel für den Zugriff auf das Laufwerk verwenden, nachdem sie aus der Benutzerliste gelöscht wurden. Bei der Umschlüsselung des Laufwerks wird dieser zugrunde liegende Schlüssel geändert und ein derartiger unberechtigter Eingriff verhindert.

So schlüsseln Sie ein PGP Virtual Disk-Laufwerk um

1. Klicken Sie im linken Fensterbereich des Hauptbildschirms von PGP Desktop auf das Bedienfeld „PGP Disk“ und wählen Sie das PGP Virtual Disk-Laufwerk aus, das Sie umschlüsseln möchten.
2. Wenn das PGP Virtual Disk-Laufwerk, das Sie umschlüsseln möchten, aktiviert ist, deaktivieren Sie es.
3. Wählen Sie das PGP Virtual Disk-Laufwerk aus, das Sie umschlüsseln möchten.
4. Klicken Sie auf **Laufwerk > Umschlüsseln**.
5. Geben Sie die Passphrase für das Laufwerk ein. Der Assistent für die Umschlüsselung des PGP-Laufwerks wird angezeigt.
6. Lesen Sie die einführenden Informationen und klicken Sie auf **Weiter**. Ein Dialogfeld mit folgenden Informationen wird anzeigt:
   - Der aktuelle Verschlüsselungsalgorithmus, mit dem das PGP Virtual Disk-Laufwerk geschützt ist.
   - Die verfügbaren Verschlüsselungsalgorithmen mit Ausnahme des Algorithmus, den Sie ursprünglich ausgewählt haben.

   Wenn das PGP Virtual Disk-Laufwerk derzeit beispielsweise mit AES verschlüsselt ist, werden in der Liste **Neuer Algorithmus** die Optionen **CAST5** und **Twofish** angezeigt.
7. Führen Sie einen der folgenden Schritte aus:
   - Umschlüsseln Sie das Laufwerk mit dem aktuellen Algorithmus, indem Sie das Kontrollkästchen **Mit demselben Algorithmus umschlüsseln** aktivieren und auf **Weiter** klicken. Das PGP Virtual Disk-Laufwerk wird mit dem gleichen Verschlüsselungsalgorithmus wie zuvor umgeschlüsselt.
   - Umschlüsseln Sie das Laufwerk mit einem anderen Algorithmus, indem Sie den Algorithmus aus dem Menü **Neuer Algorithmus** auswählen und auf **Weiter** klicken. Das PGP Virtual Disk-Laufwerk wird mit dem neuen Verschlüsselungsalgorithmus umgeschlüsselt, den Sie ausgewählt haben.
8. Wenn der aktuelle Status „Fertig“ lautet, klicken Sie auf **Weiter**.
9. Klicken Sie auf **Beenden**, um die Umschlüsselung abzuschließen.

Mit anderen Benutzern arbeiten

In diesem Abschnitt wird beschrieben, wie Konten anderer Benutzer für PGP Virtual Disk-Laufwerke hinzugefügt, gelöscht und deaktiviert werden. Darüber hinaus finden Sie hier Informationen zum Ändern der Rechte von Benutzern, einschließlich der Gewährung von Administratorrechten für einen Benutzer.

Konten anderer Benutzer zu einem PGP Virtual Disk-Laufwerk hinzufügen

Der Administrator eines PGP Virtual Disk-Laufwerks kann das Laufwerk anderen Benutzern zugänglich machen. Diese Benutzer können dann mit ihrer eigenen Passphrase oder ihrem eigenen privaten Schlüssel auf das Laufwerk zugreifen.

Stellen Sie sicher, dass das PGP Virtual Disk-Laufwerk derzeit *nicht* aktiviert ist, da ansonsten keine Konten anderer Benutzer hinzugefügt werden können.

So fügen Sie einem PGP Virtual Disk-Laufwerk Konten anderer Benutzer hinzu

1. Klicken Sie im linken Fensterbereich des Hauptbildschirms von PGP Desktop auf das Bedienfeld „PGP Disk“ und wählen Sie das PGP Virtual Disk-Laufwerk aus, dem Sie das Konto eines anderen Benutzers hinzufügen möchten.
2. Führen Sie einen der folgenden Schritte aus:
   - Fügen Sie einen neuen Benutzer eines öffentlichen Schlüssels hinzu, indem Sie auf **Benutzerschlüssel hinzufügen** klicken. Das Dialogfeld „Schlüsselbenutzer hinzufügen“ wird angezeigt.
   - Fügen Sie einen neuen Passphrasenbenutzer hinzu, indem Sie auf **Neuer Passphrasenbenutzer** klicken. Das Dialogfeld „Neuer PGP Disk-Benutzer“ wird angezeigt.
3. Führen Sie einen der folgenden Schritte aus:
   - Wenn Sie **Benutzerschlüssel hinzufügen** ausgewählt haben, wählen Sie im Dialogfeld „Schlüsselbenutzer hinzufügen“ einen öffentlichen Benutzer aus der Liste aus und klicken auf **OK**.
   - Wenn Sie **Neuer Passphrasenbenutzer** ausgewählt haben, geben Sie im Dialogfeld „Neuer PGP Disk-Benutzer“ den Benutzernamen und die Passphrase für das PGP Virtual Disk-Laufwerk ein, dem Sie den Benutzer hinzufügen. Geben Sie die Passphrase im Feld „Neuer PGP Disk-Benutzer“ erneut ein und klicken Sie auf **OK**.

   Das Konto eines anderen Benutzers wird hinzugefügt.

Konten anderer Benutzer von einem PGP Virtual Disk-Laufwerk löschen

Gelegentlich kann es erforderlich sein, einem Benutzer den Zugriff auf ein PGP Virtual Disk-Laufwerk zu entziehen.

Stellen Sie sicher, dass das PGP Virtual Disk-Laufwerk *nicht* aktiviert ist. Sie können das Konto eines anderen Benutzers nicht entfernen, wenn das Laufwerk aktiviert ist.

So entfernen Sie das Konto eines anderen Benutzers von einem PGP Virtual Disk-Laufwerk

1. Klicken Sie im linken Fensterbereich des Hauptbildschirms von PGP Desktop auf das Bedienfeld „PGP Disk“ und wählen Sie das PGP Virtual Disk-Laufwerk für das zu löschende Benutzerkonto aus.
2. Wählen Sie in der Liste „Benutzerzugriff“ den Namen des anderen Benutzers aus, dessen Konto Sie entfernen möchten. Der Administrator kann nicht entfernt werden.
3. Klicken Sie auf **Benutzer löschen**. Das Dialogfeld „Passphrase“ wird angezeigt und Sie werden zur Eingabe der Administratorpassphrase oder der Passphrase für das zu entfernende Benutzerkonto aufgefordert.
4. Geben Sie die Passphrase ein und klicken Sie auf **OK**. Das Konto des anderen Benutzers wird entfernt.

Konten anderer Benutzer deaktivieren und aktivieren

Sie können den Zugriff eines Benutzers auf ein PGP Virtual Disk-Laufwerk vorübergehend verhindern, ohne dessen Konto komplett zu entfernen, indem Sie stattdessen das Konto deaktivieren.

Stellen Sie sicher, dass das PGP Virtual Disk-Laufwerk *nicht* aktiviert ist. Sie können das Konto eines anderen Benutzers weder deaktivieren noch aktivieren, wenn das Laufwerk aktiviert ist.

So deaktivieren oder aktivieren Sie Konten anderer Benutzer auf einem PGP Virtual Disk-Laufwerk

1. Klicken Sie im linken Fensterbereich des Hauptbildschirms von PGP Desktop auf das Bedienfeld „PGP Disk“ und wählen Sie das PGP Virtual Disk-Laufwerk für das zu ändernde Benutzerkonto aus.
2. Führen Sie in der Liste „Benutzerzugriff“ einen der folgenden Schritte aus:

- Wenn Sie einen Benutzer deaktivieren möchten, klicken Sie mit der rechten Maustaste auf den Namen des zu deaktivierenden Kontos des anderen Benutzers und wählen **Deaktivieren** aus. Das Dialogfeld „Passphrase“ wird angezeigt und Sie werden zur Eingabe der Administratorpassphrase oder der Passphrase für das zu deaktivierende Benutzerkonto aufgefordert. Geben Sie die Passphrase ein und klicken Sie auf **OK**. Das Konto des anderen Benutzers wird deaktiviert.
- Wenn Sie einen zuvor deaktivierten Benutzer wieder aktivieren möchten, klicken Sie mit der rechten Maustaste auf den Namen des Kontos des anderen Benutzers, das Sie aktivieren möchten, und wählen **Aktivieren** aus. Das Dialogfeld „Passphrase“ wird angezeigt und Sie werden zur Eingabe der Administratorpassphrase oder der Passphrase für das zu aktivierende Benutzerkonto aufgefordert. Geben Sie die Passphrase ein und klicken Sie auf **OK**. Das Konto des anderen Benutzers wird aktiviert.

Lese-/Schreib- und Schreibschutzstatus ändern

Benutzer von PGP Virtual Disk-Laufwerken können entweder über vollständigen Lese-/Schreibzugriff oder nur über Lesezugriff verfügen. Diese Berechtigung kann jederzeit für Benutzer geändert werden.

Vergewissern Sie sich, dass das ausgewählte PGP Virtual Disk-Laufwerk nicht aktiviert ist. Sie können Rechte nicht ändern, wenn das Laufwerk aktiviert ist.

So ändern Sie die Rechte für einen Benutzer eines PGP Virtual Disk-Laufwerks

1. Klicken Sie im linken Fensterbereich des Hauptbildschirms von PGP Desktop auf das Bedienfeld „PGP Disk“ und wählen Sie das PGP Virtual Disk-Laufwerk für das zu ändernde Benutzerkonto aus.
2. Wählen Sie in der Liste „Benutzerzugriff“ den Namen des Benutzers aus, dessen Status geändert werden soll.
3. Führen Sie einen der folgenden Schritte aus:
   - Wenn der Benutzer nur über Leseberechtigungen verfügen soll, klicken Sie mit der rechten Maustaste auf den Benutzernamen und wählen **Schreibgeschützt** aus.
   - Wenn der Benutzer über Lese- und Schreibberechtigungen verfügen soll, klicken Sie mit der rechten Maustaste auf den Benutzernamen und wählen **Lesen/Schreiben** aus.

   Das Dialogfeld „Passphrase eingeben“ wird angezeigt.
4. Geben Sie die Administratorpassphrase für das PGP Virtual Disk-Laufwerk ein und klicken Sie auf **OK**. Die Rechte des ausgewählten Benutzers sind nun geändert.

Anderen Benutzern Administratorstatus gewähren

Sie können den Status eines Benutzerkontos ändern und einen anderen Benutzer als Administrator definieren.

Stellen Sie sicher, dass das PGP Virtual Disk-Laufwerk *nicht* aktiviert ist. Wenn das Laufwerk aktiviert ist, können Sie Benutzer nicht als Administrator definieren.

So gewähren Sie Administratorstatus

1. Klicken Sie im linken Fensterbereich des Hauptbildschirms von PGP Desktop auf das Bedienfeld „PGP Disk“ und wählen Sie das PGP Virtual Disk-Laufwerk für das zu ändernde Benutzerkonto aus.
2. Wählen Sie in der Liste „Benutzerzugriff“ den Benutzer aus, den Sie als Administrator für das PGP Virtual Disk-Laufwerk definieren möchten. Wählen Sie entweder einen Passphrasenbenutzer oder sich selbst (wenn Sie nicht der aktuelle Administrator sind). Beachten Sie, dass Sie keinen Benutzer eines öffentlichen Schlüssels als Administrator für das PGP Virtual Disk-Laufwerk definieren können.
3. Klicken Sie in der Optionsleiste links auf **Als Administrator definieren**. Dem ausgewählten Benutzerkonto wird der Administratorstatus zugewiesen.

Hinweis: Sie können immer nur einem Benutzerkonto den Administratorstatus zuweisen. Wenn Sie einem Konto den Administratorstatus zuweisen, wird dieser Status automatisch von einem anderen Konto entfernt.

Benutzer-Passphrasen ändern

Stellen Sie sicher, dass das PGP Virtual Disk-Laufwerk *nicht* aktiviert ist. Sie können die Passphrase nicht ändern, wenn das Laufwerk aktiviert ist.

So ändern Sie die Passphrasen eines Benutzers für ein PGP Virtual Disk-Laufwerk

1. Klicken Sie im linken Fensterbereich des Hauptbildschirms von PGP Desktop auf das Bedienfeld „PGP Disk“ und wählen Sie das PGP Virtual Disk-Laufwerk aus, für das Sie ein Benutzer sind.
2. Wählen Sie den Namen eines Passphrasenbenutzers aus der Liste „Benutzerzugriff“ aus und klicken Sie auf **Passphrase ändern**. Das Dialogfeld „Passphrase eingeben“ wird angezeigt.

Tipp: Sie können auch mit der rechten Maustaste auf den Benutzernamen klicken und im Kontextmenü die Option **Benutzerpassphrase ändern** auswählen.

3 Geben Sie die aktuelle Passphrase für den Benutzer ein und klicken Sie auf **OK**. Das Dialogfeld „Bestätigte PGP-Passphrase eingeben“ wird angezeigt.

4 Geben Sie eine neue Passphrase ein. Geben Sie sie zur Bestätigung erneut ein und klicken Sie auf **OK**. Die Passphrase wird geändert.

PGP Virtual Disk-Laufwerke löschen

Möglicherweise stellen Sie irgendwann fest, dass Sie ein bestimmtes PGP Virtual Disk-Laufwerk nicht mehr benötigen und entscheiden sich, das gesamte Laufwerk zu löschen.

Achtung: Beim Löschen eines PGP Virtual Disk-Laufwerks werden auch alle darauf befindlichen Daten gelöscht. *Es gibt keine Möglichkeit, die Daten wiederherzustellen, nachdem ein PGP Virtual Disk-Laufwerk gelöscht wurde*. Stellen Sie sicher, dass Sie alle Daten, die Sie speichern möchten, an einen anderen Speicherort kopiert haben, *bevor Sie ein PGP Virtual Disk-Laufwerk löschen*.

Stellen Sie sicher, dass das PGP Virtual Disk-Laufwerk *nicht* aktiviert ist. Ein aktiviertes PGP Virtual Disk-Laufwerk kann nicht gelöscht werden.

So löschen Sie ein PGP Virtual Disk-Laufwerk

1 Klicken Sie im linken Fensterbereich des Hauptbildschirms von PGP Desktop auf das Bedienfeld „PGP Disk“ und wählen Sie das PGP Virtual Disk-Laufwerk aus, das Sie löschen möchten.

2 Klicken Sie auf **Laufwerk > löschen**. Ein Bestätigungsdialogfeld wird angezeigt.

3 Führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf **OK**, um das PGP Virtual Disk-Laufwerk aus der PGP Desktop-Liste zu entfernen. Das PGP Virtual Disk-Laufwerk verbleibt auf dem System.
- Klicken Sie auf **PGP-Laufwerk löschen**, um das PGP Virtual Disk-Laufwerk aus der PGP Desktop-Liste zu entfernen und gleichzeitig von der Festplatte zu löschen.

PGP Virtual Disk-Laufwerke warten

In diesem Abschnitt wird die ordnungsgemäße Handhabung von PGP Virtual Disk-Laufwerken beschrieben, die Sie mit Ihrem Computer verwenden.

PGP Virtual Disk-Laufwerke auf einem Remoteserver aktivieren

PGP Virtual Disk-Laufwerke können auf jeder Art von Server (Windows oder UNIX) platziert werden. Die Laufwerke können dann von jedem Benutzer mit einem Windows-Computer und PGP Desktop aktiviert werden.

Hinweis: Die erste Person, die das PGP Virtual Disk-Laufwerk lokal aktiviert, erhält Lese-/Schreibzugriff auf das Laufwerk. Danach können keine weiteren Personen auf das Laufwerk zugreifen. Wenn Sie den Zugriff durch andere Personen zulassen möchten, müssen Sie das Laufwerk im schreibgeschützten Modus aktivieren (gilt nur für FAT- und FAT32-Dateisysteme). Alle Benutzer des Laufwerks verfügen dann ausschließlich über Lesezugriff.

Wenn das PGP Virtual Disk-Laufwerk auf einem Windows-Server gespeichert ist, können Sie das Laufwerk auch remote auf dem Server aktivieren und anderen Personen die Freigabe des aktivierten Laufwerks gestatten. Dieses Verfahren bietet jedoch keinen Schutz für die Dateien auf dem Laufwerk.

Sicherungskopien von PGP Virtual Disk-Laufwerken erstellen

Sie können Daten am besten vor Hardwarefehlern oder sonstigem Verlust schützen, indem Sie Sicherungskopien des Inhalts der PGP Virtual Disk-Laufwerke erstellen.

Es empfiehlt sich nicht, den Inhalt eines aktivierten (und daher entschlüsselten) PGP Virtual Disk-Laufwerks wie jedes andere Laufwerk zu sichern. Der Inhalt ist nicht verschlüsselt und daher für jeden zugänglich, der die Sicherungskopie wiederherstellen kann. Erstellen Sie stattdessen eine Sicherungskopie des verschlüsselten Laufwerks.

So sichern Sie PGP Virtual Disk-Laufwerke

1. Deaktivieren Sie das PGP Virtual Disk-Laufwerk.
2. Kopieren Sie die deaktivierte verschlüsselte Datei auf eine Diskette, ein Band oder ein Steckmodul. Selbst wenn eine unbefugte Person Zugriff auf die Sicherungsdatei erhält, kann sie den Inhalt nicht entschlüsseln.

Beachten Sie beim Erstellen von Sicherungskopien verschlüsselter Dateien folgende Hinweise:

- Das Erstellen von Sicherungskopien der verschlüsselten Dateien auf einem Netzlaufwerk bietet anderen Personen ausreichend Gelegenheit, eine schwache Passphrase zu erraten. Es ist bedeutend sicherer, Sicherungskopien nur auf Geräten zu erstellen, die sich physisch in Ihrem Besitz befinden.
- Eine lange und komplizierte Passphrase verbessert die Sicherheit Ihrer Daten zusätzlich.
- Wenn Sie in einem Netzwerk arbeiten, achten Sie darauf, dass die Dateien auf Ihrem *aktivierten* PGP Virtual Disk-Laufwerk nicht durch ein Netzwerksicherungssystem gesichert werden. (Wenden Sie sich ggf. an den Systemadministrator.) Nach der Aktivierung eines PGP Virtual Disk-Laufwerks sind dessen Dateien entschlüsselt und können auf ein Netzwerksicherungssystem kopiert werden.

PGP Virtual Disk-Laufwerke austauschen

Sie können PGP Virtual Disk-Laufwerke mit anderen Benutzern austauschen, die auf ihren Computern PGP Desktop installiert haben. Dazu senden Sie diesen Personen eine Kopie der Datendatei des PGP Virtual Disk-Laufwerks, die die Laufwerksdaten enthält. PGP Virtual Disk-Laufwerke können u. a. folgendermaßen ausgetauscht werden:

- Als E-Mail-Anlagen
- Auf einem Wechseldatenträger oder auf CDs
- Über ein Netzwerk

Nachdem der andere Benutzer die PGP Virtual Disk-Laufwerksdatei erhalten hat, kann dieser sie auf einem System mit PGP Desktop aktivieren und unter Verwendung der richtigen Passphrase darauf zugreifen. Wenn das Laufwerk an ihren öffentlichen Schlüssel verschlüsselt wurde, würden sie ihren privaten Schlüssel für den Zugriff verwenden.

Hinweis: Der öffentliche Schlüssel ist aus folgenden Gründen die sicherste Schutzmethode beim Hinzufügen anderer Benutzer zu einem PGP Virtual Disk-Laufwerk: (1) Sie müssen keine Passphrase mit dem anderen Benutzer austauschen, die, abhängig von der Austauschmethode, abgefangen oder abgehört werden könnte. (2) Der andere Benutzer muss sich keine weitere Passphrase merken, die er vergessen könnte. (3) Die Verwaltung einer Liste von Benutzern wird vereinfacht, wenn jeder Benutzer einen eigenen privaten Schlüssel zum Entsperren des Laufwerks verwendet.

PGP Virtual Disk-Verschlüsselungsalgorithmen

Bei der Verschlüsselung wird eine mathematische Formel zum Chiffrieren von Daten eingesetzt, damit sie von anderen Personen nicht verwendet werden können. Wenn Sie den richtigen mathematischen Schlüssel anwenden, werden die Daten wieder dechiffriert. Die Verschlüsselungsformel für PGP Virtual Disk-Laufwerke verwendet für einen Teil des Verschlüsselungsvorgangs Zufallsdaten.

Die PGP Desktop-Anwendung bietet starke Algorithmusoptionen zum Schutz von PGP Virtual Disk-Laufwerken: AES-256, CAST und Twofish.

- Der erweiterte Verschlüsselungsstandard AES (Advanced Encryption Standard) ist der von NIST genehmigte Verschlüsselungsstandard. Der zugrunde liegende Algorithmus ist Rijndael, ein von Joan Daemen und Vincent Rijmen entwickelter Block-Algorithmus. AES ersetzt den vorherigen Datenverschlüsselungsstandard DES (Data Encryption Standard). PGP Virtual Disk-Laufwerke können mit der stärksten Variation von AES, AES-256 (d. h. AES mit einer Schlüsselgröße von 256 Bit) geschützt werden.
- CAST gilt als ausgezeichneter Block-Algorithmus, da er schnell auszuführen, jedoch nur schwer zu entziffern ist. Der Name ist von den Initialen der Entwickler Carlisle Adams und Stafford Tavares von Northern Telecom (Nortel) abgeleitet. Nortel hat ein Patent für CAST angemeldet, verpflichtet sich jedoch, CAST ohne Lizenzgebühren für jedermann verfügbar zu machen. Bei CAST scheint es sich um einen Algorithmus zu handeln, der von Spezialisten mit hervorragendem Ruf innerhalb der Branche außergewöhnlich gut entwickelt wurde.

  Das Design basiert auf einem sehr formellen Ansatz und enthält eine Reihe formal nachweisbarer Behauptungen, die Grund zu der Annahme geben, dass alle Schlüssel geprüft werden müssten, bevor der 128-Bit-Schlüssel entziffert würde. CAST hat keine schwachen Schlüssel. Es gibt überzeugende Argumente dafür, dass CAST gegen lineare und differenziale Kryptanalyse immun ist, die zwei leistungsstärksten Formen von Kryptanalyse in der veröffentlichten Literatur. Beide haben sich beim Knacken von DES als effektiv erwiesen.
- Twofish ist ein relativ neuer, jedoch sehr geschätzter symmetrischer Block-Algorithmus mit 256 Bit. Twofish gehörte zu fünf Algorithmen, die das U.S. National Institute of Standards and Technology (NIST) für den neuen erweiterten Verschlüsselungsstandard (AES) in Betracht gezogen hatte.

Spezielle Sicherheitsfunktionen von PGP Virtual Disk

Im Gegensatz zu manchen anderen Programmen legt PGP Desktop besonderen Wert auf die Vermeidung von Sicherheitsproblemen mit PGP Virtual Disk-Laufwerken.

Diese Sicherheitsmaßnahmen gelten auch für vollständig verschlüsselte Laufwerke.

Löschung der Passphrase

Wenn Sie eine Passphrase eingeben, wird diese von PGP Desktop nur für kurze Zeit verwendet und danach aus dem Speicher gelöscht. PGP Desktop erstellt außerdem keine Kopien der Passphrase. Daher befindet sich die Passphrase in der Regel nur für den Bruchteil einer Sekunde im Speicher. Diese Funktion ist von größter Bedeutung, da sonst andere Personen im Hauptspeicher nach der Passphrase suchen könnten, während Sie nicht an Ihrem Arbeitsplatz sind. Diese Personen würden dann ohne Ihr Wissen vollständigen Zugriff auf alle mit dieser Passphrase geschützten Daten erhalten.

Schutz des virtuellen Speichers

Ihre Passphrase oder andere Schlüssel könnten mit den Daten des virtuellen Speichersystems auf die Festplatte ausgelagert werden. PGP Desktop lässt jedoch nicht zu, dass die Passphrasen und Schlüssel auf die Festplatte geschrieben werden. Mit dieser Funktion wird verhindert, dass unberechtigte Personen die virtuelle Speicherdatei nach Passphrasen durchsuchen.

Ruhezustand

Unter Windows wird beim Wechsel in den Ruhezustand ein Image des gesamten Hauptspeichers des Computers, einschließlich der PGP Virtual Disk-Laufwerksinformationen, in eine Datei auf der Festplatte geschrieben. Wenn das PGP Virtual Disk-Laufwerk bei der Aktivierung des Ruhezustands geöffnet ist, werden vertrauliche Daten (auch der Sitzungsschlüssel, jedoch *nicht* die Passphrase) auf der Festplatte gespeichert.

Da der Ruhezustand des Computers nicht sicher ist, empfiehlt die PGP Corporation, eine Verschlüsselung mit PGP Whole Disk Encryption durchzuführen oder sicherzustellen, dass in den PGP-Optionen auf der Registerkarte „Laufwerk“ die PGP Virtual Disk-Optionen **Deaktivieren im Standbymodus** und **Standbymodus verhindern, wenn PGP-Laufwerke nicht deaktiviert werden können** aktiviert sind.

Schutz durch MSIM (Memory Static Ion Migration)

Wenn Sie ein PGP Virtual Disk-Laufwerk aktivieren, wird die Passphrase in einen Schlüssel umgewandelt. Dieser Schlüssel dient zum Verschlüsseln und Entschlüsseln der Daten auf dem PGP Virtual Disk-Laufwerk. Obwohl die Passphrase sofort aus dem Speicher gelöscht wird, bleibt der Schlüssel (aus dem die Passphrase nicht abgeleitet werden kann) jedoch im Speicher erhalten, während das Laufwerk aktiviert ist.

Dieser Schlüssel wird zwar nicht im virtuellen Speicher gespeichert, wenn jedoch ein bestimmter Speicherbereich genau dieselben Daten für extrem lange Zeiträume speichert, ohne dass der Computer ausgeschaltet oder zurückgesetzt wird, bleibt eine statische Ladung im Speicher zurück, die von Angreifern gelesen werden könnte. Wenn das PGP Virtual Disk-Laufwerk für längere Zeit aktiviert bleibt, können mit der Zeit erkennbare Spuren des Schlüssels im Speicher zurückbleiben. Mit bestimmten Geräten könnte der Schlüssel wiederhergestellt werden. Diese Geräte sind zwar nicht im Elektronikfachgeschäft um die Ecke zu finden, stehen wahrscheinlich jedoch größeren Regierungsbehörden zur Verfügung.

PGP Desktop schützt vor derartigen Angriffen, indem zwei Kopien (eine normale Kopie und eine Kopie mit umgekehrten Bit) im RAM-Speicher gehalten und alle paar Sekunden umgekehrt werden.

Weitere Sicherheitsaspekte

Im Allgemeinen hängt die Fähigkeit zum Schützen von Daten von den Vorkehrungen ab, die Sie treffen. Kein Verschlüsselungsprogramm kann Sie vor unzureichenden Sicherheitsmaßnahmen schützen. Wenn Sie sich z. B. vom Schreibtisch entfernen und dabei den Computer eingeschaltet und vertrauliche Dateien geöffnet lassen, kann jeder auf die Informationen zugreifen oder sogar den Schlüssel für den Zugriff auf die Daten erhalten.

Im Folgenden sind einige Empfehlungen zur Wahrung der optimalen Sicherheit aufgeführt:

- Deaktivieren Sie PGP Virtual Disk-Laufwerke, bevor Sie sich vom Computer entfernen. Die Dateien werden dann sicher in der verschlüsselten Datei gespeichert, die dem Laufwerk zugeordnet ist, bis Sie erneut darauf zugreifen möchten.
- Verwenden Sie einen Bildschirmschoner mit Kennwortschutz, um anderen Personen den Zugriff auf den Computer oder das Anzeigen des Bildschirms zu erschweren, wenn Sie sich nicht am Schreibtisch befinden.
- Stellen Sie sicher, dass die PGP Virtual Disk-Laufwerke nicht für andere Computer im Netzwerk freigegeben werden. Wenden Sie sich dazu ggf. an den Netzwerkadministrator. Die Dateien in einem aktivierten PGP Virtual Disk-Laufwerk sind für alle Personen zugänglich, die sie im Netzwerk sehen können.
- Schreiben Sie Ihre Passphrasen auf keinen Fall auf. Wählen Sie eine Passphrase, die Sie sich merken können. Wenn Sie sich die Passphrase nur schwer merken können, verwenden Sie eine Gedächtnisstütze (z. B. Poster, Lieder, Gedichte oder Witze), aber *schreiben Sie die Passphrasen nicht auf*.
- Wenn Sie PGP Desktop zu Hause einsetzen und den Computer gemeinsam mit anderen Personen verwenden, können diese wahrscheinlich Ihre PGP Virtual Disk-Laufwerksdateien sehen. Deaktivieren Sie daher die nicht benötigten PGP Virtual Disk-Laufwerke, damit ihr Inhalt nicht von anderen Personen gelesen werden kann.

- Wenn eine andere Person physisch Zugriff auf Ihren Computer hat, kann diese Person Ihre PGP Virtual Disk-Laufwerksdateien sowie andere Dateien oder Laufwerke löschen. Wenn der physische Zugriff ein Problem darstellt, sichern Sie die PGP Virtual Disk-Laufwerksdateien oder speichern Sie sie auf einem externen Gerät, auf das nur Sie Zugriff haben.
- Beachten Sie, dass die Kopien des PGP Virtual Disk-Laufwerks denselben Verschlüsselungsschlüssel verwenden wie das Original. Wenn Sie eine Kopie des Laufwerks mit einer anderen Person austauschen und Sie beide Ihre Hauptkennwörter ändern, wird weiterhin derselbe Schlüssel zur Verschlüsselung der Daten verwendet. Der Schlüssel kann dann zwar wiederhergestellt werden, dies ist jedoch nicht einfach.

  Sie können den zugrunde liegenden Schlüssel durch Umschlüsselung des Laufwerks ändern.

12 Mobile Daten mit PGP Portable erstellen und darauf zugreifen

Mit PGP Portable können Sie verschlüsselte Dateien an Benutzer weitergeben, die nicht über PGP Desktop verfügen. Verwenden Sie PGP Portable, um Dateien sicher an andere Systeme weiterzugeben, auf denen keine PGP-Software installiert ist oder installiert werden kann.

PGP Portable bietet folgende Vorteile:

- Transportierbarkeit gesicherter Dokumente
- Einfache Verteilung gesicherter Dokumente

PGP Portable wird von zwei Arten von Benutzern verwendet: von dem Benutzer, der das PGP Portable-Laufwerk mit den gesicherten Daten erstellt, und von dem Benutzer, der nicht über PGP-Software verfügt, aber auf die gesicherten Daten zugreifen muss. Sie können auch zu beiden Arten von Benutzern gehören. Dies wäre beispielsweise der Fall, wenn Sie ein PGP Portable-Laufwerk erstellen, das Sie zu einem Kunden mitnehmen und dort auf einem Computer verwenden.

Unter Windows können Sie PGP Portable-Laufwerke erstellen und auf die verschlüsselten Daten zugreifen.

In diesem Kapitel

PGP Portable-Laufwerke erstellen..... 241
Auf Daten auf einem PGP Portable-Laufwerk zugreifen 245

PGP Portable-Laufwerke erstellen

Es gibt zwei Möglichkeiten, PGP Portable-Laufwerke zu erstellen: mithilfe eines Kontextmenüs von Windows Explorer oder mithilfe eines Befehlszeilenprogramms. In diesem Abschnitt wird die normale Verwendung des Kontextmenüs beschrieben. Informationen zur Befehlszeile finden Sie unter PGP Portable-Befehlszeilenprogramm verwenden.

Voraussetzungen für die Erstellung eines PGP Portable-Laufwerks:

- PGP Portable muss auf einem Windows-System installiert sein, auf dem bereits PGP Desktop ausgeführt wird.

- Die an einen PGP Universal Server gebundene PGP Desktop-Installation muss ordnungsgemäß lizenziert sein.

PGP Portable-Laufwerke können auf zwei Zielmedien erstellt werden:

- Einem Ordner auf einem lokalen Laufwerk, einer Remote-Dateifreigabe oder einer CD/DVD
- Einem lokal aktivierten Wechseldatenträger, z. B. einem USB-Flash-Laufwerk, mit einer Größe von maximal 128 GB

Wenn Sie ein PGP Portable-Laufwerk erstellen, wird durch die PGP Universal Server-Richtlinie auch die Stärke der Passphrase durchgesetzt. Falls die verwendete Passphrase nicht der PGP Universal Server-Richtlinie entspricht, wird eine Fehlermeldung angezeigt.

PGP Portable-Laufwerk von einem Ordner erstellen

Verwenden Sie diese Option, wenn Sie eine CD oder DVD mit dem PGP Portable-Laufwerk brennen möchten.

Hinweis: Vergewissern Sie sich, dass Sie die Daten, die Sie schützen und freigeben möchten, in den Ordner kopiert haben.

So erstellen Sie ein PGP Portable-Laufwerk von einem Ordner

1. Klicken Sie mit der rechten Maustaste auf den Quellordner und wählen Sie aus dem Kontextmenü die Option **Ordner für PGP Portable-Laufwerk erstellen** aus.
2. Geben Sie im Dialogfeld „PGP Portable-Laufwerk erstellen“ die Passphrase ein und bestätigen Sie sie. Diese Passphrase wird für den Zugriff auf die Daten im PGP Portable-Laufwerk benötigt.
3. Klicken Sie auf **Erstellen**.
   - Wenn sich der Ordner, den Sie für die Erstellung des PGP Portable-Laufwerks verwenden, auf einem schreibgeschützten Speichermedium (z. B. einer CD oder DVD) befindet, wird das Dialogfeld „Speichern unter“ angezeigt. Wechseln Sie zu dem Speicherort auf dem lokalen Laufwerk, an dem Sie den Zielordner für das PGP Portable-Laufwerk erstellen möchten, und klicken Sie auf **Speichern**.

   Der Zielordner wird erstellt. Der Ordnername setzt sich aus dem Namen des Quellordners mit dem Anhang „- PGP Portable“ zusammen.
4. Brennen Sie den gesamten Inhalt des Zielordners auf die CD/DVD. Der Zielordner des PGP Portable-Laufwerks enthält folgende Dateien:
   - Die ausführbare Windows-Datei von PGP Portable (`pgpportable.exe`)

- Die ausführbaren Mac OS X-Dateien von PGP Portable (`PGP Portable App`)
- Eine Autorun-Datei von Windows (`autorun.inf`)
- Eine PGP Portable-Laufwerksdatei (`pgpportable.pgd`)

Die PGP Portable-Laufwerksdatei (`pgpportable.pgd`) enthält alle Dateien aus dem ursprünglichen Zielordner. Die PGP Portable-Laufwerksdatei ist an die angegebene Passphrase verschlüsselt.

Achten Sie darauf, dass Sie keine dieser Dateien vom PGP Portable-Laufwerk löschen.

Tipp: Stellen Sie sicher, dass Sie lediglich den Inhalt des Ordners auf die CD/DVD brennen und nicht den Ordner selbst. Wenn Sie den Ordner auf die CD/DVD brennen, kann PGP Portable auf Systemen mit aktivierter Autorun-Funktion nicht automatisch gestartet werden.

PGP Portable-Laufwerk von einem USB-Wechseldatenträger erstellen

Verwenden Sie diese Option, wenn Sie das PGP Portable-Laufwerk direkt auf einem USB-Wechseldatenträger, z. B. einem Flash-Laufwerk, erstellen möchten.

Hinweis: Die Größe des USB-Wechseldatenträgers muss unter 128 GB (137438953472 Byte) liegen. Wenn Sie versuchen, ein PGP Portable-Laufwerk auf einem USB-Wechseldatenträger mit einer Größe von mehr als 128 GB zu erstellen, wird eine Fehlermeldung ausgegeben.

So erstellen Sie ein PGP Portable-Laufwerk von einem USB-Wechseldatenträger

1. Klicken Sie mit der rechten Maustaste auf den aktivierten USB-Wechseldatenträger und wählen Sie aus dem Kontextmenü die Option **PGP Portable-Laufwerk erstellen** aus.
2. Die Anwendung zum Erstellen von PGP Portable-Laufwerken wird mit einer Warnmeldung angezeigt, dass der Inhalt des Laufwerks gelöscht wird.
3. Geben Sie im Dialogfeld „PGP Portable-Laufwerk erstellen“ die Passphrase ein und bestätigen Sie sie. Diese Passphrase wird für den Zugriff auf die Daten im PGP Portable-Laufwerk benötigt.
4. Klicken Sie auf **Formatieren**. Nach Abschluss der Formatierung wird das PGP Portable-Laufwerk erstellt. Die PGP Portable-Laufwerksdatei ist an die angegebene Passphrase verschlüsselt.
5. Sie werden zur Eingabe der Passphrase aufgefordert. Anschließend wird das PGP Portable-Laufwerk aktiviert. In der Taskleiste wird eine Benachrichtigung mit der Laufwerksnummer des aktivierten PGP Portable-Laufwerks angezeigt.

6 Sie können nun die Daten, die Sie schützen möchten, auf das aktivierte PGP Portable-Laufwerk kopieren. Wenn das PGP Portable-Laufwerk zum ersten Mal erstellt wird, enthält es keine Dateien.

7 Deaktivieren Sie das PGP Portable-Laufwerk (klicken Sie in der Taskleiste auf das PGP Portable-Symbol und wählen Sie **Deaktivieren und beenden** aus). Das für das PGP Portable-Laufwerk aktivierte Laufwerk wird deaktiviert.

8 Entfernen Sie das USB-Gerät ordnungsgemäß vom Computer. Sie können jetzt auf einem anderen System, das PGP Portable unterstützt, auf den Inhalt des PGP Portable-Laufwerks zugreifen.

Warnung: Vergewissern Sie sich, dass Sie einen USB-Wechseldatenträger ordnungsgemäß deaktivieren, bevor Sie ihn physisch vom System entfernen. Andernfalls kann der Dateiinhalt beschädigt werden.

Der Wechseldatenträger enthält die folgenden Dateien:

- Die ausführbare Windows-Datei von PGP Portable (`pgpportable.exe`)
- Die ausführbaren Mac OS X-Dateien von PGP Portable (`PGP Portable App`)
- Eine Autorun-Datei von Windows (`autorun.inf`)
- Die PGP Portable-Laufwerksdatei (`pgpportable.pgd`)

Achten Sie darauf, dass Sie keine dieser Dateien vom PGP Portable-Laufwerk löschen.

PGP Portable-Laufwerke mit Lese-/Schreibzugriff oder Schreibschutz erstellen

Damit Sie Lese-/Schreibzugriff auf ein PGP Portable-Laufwerk haben, muss sich das PGP Portable-Laufwerk auf einem Medium mit Lese-/Schreibzugriff befinden (z. B. einem Flash-Laufwerk oder einem anderen Wechseldatenträger). Der Lese-/Schreibzugriff ist für ein PGP Portable-Laufwerk nur so lange aktiviert, wie es sich auf dem Wechseldatenträger befindet, auf dem es erstellt wurde.

- PGP Portable-Laufwerke, die auf schreibgeschützten Medien (z. B. CD-ROMs) erstellt wurden, sind selbst auch schreibgeschützt.
- PGP Portable-Laufwerke, auf die über den Wechseldatenträger zugegriffen wird, auf dem sie erstellt wurden, sind mit Lese-/Schreibzugriff versehen (z. B. ein USB-Laufwerk, das mit Lese-/Schreibzugriff aktiviert wurde).

Auf Daten auf einem PGP Portable-Laufwerk zugreifen

Es gibt drei Möglichkeiten, auf den Inhalt eines PGP Portable-Laufwerks zuzugreifen:

- Durch Aktivieren der CD, DVD bzw. des USB-Wechseldatenträgers unter Windows und Ausführen von PGP Portable (die Anwendung wird bei aktivierter Autorun-Funktion automatisch gestartet).
- Durch Aktivieren der CD, DVD bzw. des USB-Wechseldatenträgers unter Mac OS X und Ausführen von PGP Portable.

Beachten Sie beim Zugriff auf die Daten auf einem PGP Portable-Laufwerk, dass Sie eigentlich zwei Teile aktivieren: den Wechseldatenträger, auf dem sich das PGP Portable-Laufwerk befindet, und das PGP Portable-Laufwerk (das separat aktiviert wird). Wenn Sie fertig sind, müssen Sie das PGP Portable-Laufwerk deaktivieren, bevor Sie den Wechseldatenträger ordnungsgemäß entfernen.

Die Schritte für den Zugriff auf die Daten auf einem PGP Portable-Laufwerk sind unter Windows und Mac OS X ähnlich.

Warnung: Vergewissern Sie sich, dass Sie einen Wechseldatenträger ordnungsgemäß deaktivieren, bevor Sie ihn physisch vom System entfernen. Andernfalls kann der Dateiinhalt beschädigt werden.

So greifen Sie unter Windows auf Daten auf einem PGP Portable-Laufwerk zu

1. Legen Sie den Wechseldatenträger ein, auf dem sich das PGP Portable-Laufwerk befindet. Es kann sich dabei um eine CD/DVD, ein Flash-Laufwerk oder einen anderen Wechseldatenträger handeln.
2. Führen Sie einen der folgenden Schritte aus:
   - Wenn unter Windows die Autorun-Funktion aktiviert ist, wählen Sie die Option **PGP Portable-Laufwerk aktivieren** aus.
   - Wenn unter Windows die Autorun-Funktion deaktiviert ist, öffnen Sie den aktivierten Wechseldatenträger und durchsuchen Sie ihn nach der PGP Portable-Anwendung (`pgpportable.exe`). Doppelklicken Sie auf die Anwendung.
   - Unter Windows 7 öffnen Sie das Laufwerk, indem Sie in Windows Explorer auf das USB-Laufwerkssymbol doppelklicken.

Das Dialogfeld „PGP Portable“ wird angezeigt.

3 Geben Sie die Passphrase für das PGP Portable-Laufwerk ein. Das PGP Portable-Laufwerk wird aktiviert.

In der Taskleiste wird eine Benachrichtigung mit der Laufwerksnummer des aktivierten PGP Portable-Laufwerks angezeigt. Wenn der Wechseldatenträger mit Lese-/Schreibzugriff aktiviert wurde, können Sie dem PGP Portable-Laufwerk Daten hinzufügen. Dies ist nicht möglich, wenn das PGP Portable-Laufwerk als schreibgeschütztes Gerät aktiviert wurde.

Hinweis: Der Laufwerksname für das PGP Portable-Laufwerk ist für PGP Portable eindeutig. Er darf nicht mit dem Namen des Laufwerks übereinstimmen.

4 Wenn Sie die Verwendung des PGP Portable-Laufwerks abgeschlossen haben, deaktivieren Sie das PGP Portable-Laufwerk (klicken Sie in der Taskleiste auf das PGP Portable-Symbol und wählen Sie **Deaktivieren und beenden** aus). Das für das PGP Portable-Laufwerk aktivierte Laufwerk wird deaktiviert.

5 Entfernen Sie das USB-Gerät bzw. die CD/DVD ordnungsgemäß vom Computer.

Passphrase für ein PGP Portable-Laufwerk ändern

Gelegentlich kann es erforderlich sein, die mit einem PGP Portable-Laufwerk verknüpfte Passphrase zu ändern. Beachten Sie, dass die Passphrase eines schreibgeschützten PGP Portable-Laufwerks nicht geändert werden kann (dies gilt auch für PGP Portable-Laufwerke, die auf CDs/DVDs gebrannt wurden).

So ändern Sie die Passphrase auf einem PGP Portable-Laufwerk unter Windows

1 Legen Sie den Wechseldatenträger ein, auf dem sich das PGP Portable-Laufwerk befindet. Es kann sich dabei um eine CD/DVD, ein Flash-Laufwerk oder einen anderen Wechseldatenträger handeln.

2 Führen Sie einen der folgenden Schritte aus:

- Wenn unter Windows die Autorun-Funktion aktiviert ist, wählen Sie die Option **PGP Portable-Laufwerk aktivieren** aus.

- Wenn unter Windows die Autorun-Funktion deaktiviert ist, öffnen Sie den aktivierten Wechseldatenträger und durchsuchen Sie ihn nach der PGP Portable-Anwendung (`pgpportable.exe`). Doppelklicken Sie auf die Anwendung.
- Unter Windows 7 öffnen Sie das Laufwerk, indem Sie in Windows Explorer auf das USB-Laufwerkssymbol doppelklicken.

3 Geben Sie bei der Aufforderung die Passphrase für das PGP Portable-Laufwerk ein. Das PGP Portable-Laufwerk wird aktiviert. In der Taskleiste wird eine Benachrichtigung mit der Laufwerksnummer des aktivierten PGP Portable-Laufwerks angezeigt.

4 Öffnen Sie PGP Portable, indem Sie mit der rechten Maustaste auf das Symbol in der Taskleiste klicken und **PGP Portable öffnen** auswählen.

5 Klicken Sie im PGP Portable-Dialogfeld auf **Passphrase ändern**.

6 Geben Sie die aktuelle Passphrase ein. Geben Sie die neue Passphrase ein, bestätigen Sie diese und klicken Sie auf **Ändern**. Die Passphrase wird geändert.

Die Passphrasen-Qualitätsanzeige kann als allgemeiner Anhaltspunkt für die Stärke der erstellten Passphrase verwendet werden. Weitere Informationen finden Sie unter *Die Passphrasen-Qualitätsanzeige* (auf Seite 352).

PGP Portable-Laufwerk deaktivieren

Vergewissern Sie sich, dass Sie einen Wechseldatenträger ordnungsgemäß deaktivieren, bevor Sie ihn physisch vom System entfernen. Andernfalls kann der Dateiinhalt beschädigt werden.

So deaktivieren Sie ein PGP Portable-Laufwerk

1 Öffnen Sie PGP Portable. Führen Sie hierzu einen der folgenden Schritte aus:

- Windows: Klicken Sie zum Öffnen von PGP Portable mit der rechten Maustaste auf das Symbol in der Taskleiste und wählen Sie **Deaktivieren und beenden** aus.
- Mac OS: Klicken Sie zum Öffnen von PGP Portable auf das Symbol im Dock und wählen Sie **Deaktivieren und beenden** aus.

Das PGP Portable-Laufwerk wird deaktiviert.

2 Entfernen Sie den Wechseldatenträger vom System.

13 PGP NetShare verwenden

PGP NetShare bietet transparente End-to-End-Verschlüsselung für die Speicherung freigegebener Dateien.

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung verwenden, hat Ihr PGP Universal Server-Administrator ggf. bestimmte Funktionen deaktiviert. Ist eine Funktion deaktiviert, wird das Bedienelement auf der linken Seite nicht angezeigt und das Menü oder andere auf diese Funktion zutreffenden Optionen sind nicht verfügbar. Die in diesem Handbuch enthaltenen Abbildungen entsprechen der Standardinstallation, bei der alle Funktionen aktiviert sind. Wenn Ihr PGP Universal Server-Administrator diese Funktion deaktiviert hat, ist dieser Abschnitt für Sie nicht relevant.

In diesem Kapitel

Informationen zu PGP NetShare 250
PGP NetShare lizenzieren 253
Schlüssel autorisierter Benutzer 254
PGP NetShare-Administratoren (Besitzer) einrichten 254
Negativ gelistete und positiv gelistete Dateien, Ordner und Anwendungen 255
Mit geschützten Ordnern arbeiten 258
Mit PGP NetShare-Benutzern arbeiten 268
PGP NetShare-Zugriffslisten importieren 272
Mit Active Directory-Gruppen arbeiten 273
Durch PGP NetShare geschützte Ordner entschlüsseln 275
Ordner umschlüsseln 276
Passphrasen löschen 277
Dateien außerhalb eines geschützten Ordners schützen 277
Sicherungskopien für durch PGP NetShare geschützte Dateien erstellen 279
Mithilfe des Kontextmenüs auf PGP NetShare-Funktionen zugreifen 280
PGP NetShare in einer von einem PGP Universal Server verwalteten Umgebung 281
Auf die Eigenschaften geschützter Dateien oder Ordner zugreifen 282
PGP NetShare-Menüs in PGP Desktop verwenden 283

Informationen zu PGP NetShare

Mit PGP NetShare können Benutzer geschützte Dateien in einem freigegebenen Speicherbereich, z. B. auf einem firmeninternen Dateiserver, in einem freigegebenen Ordner oder auf einem Wechselmedium (z. B. einem USB-Laufwerk), gemeinsam verwenden.

Hinweis: Wenn kein freigegebener, leicht zugänglicher Speicherort zur Verfügung steht, bietet ein USB-Laufwerk eine Möglichkeit für die gemeinsame Nutzung von PGP NetShare-Dateien.

Die Dateien sind durch Verschlüsselung geschützt, werden jedoch weiterhin wie normale Anwendungsdateien angezeigt (Notepad, Microsoft Word, HTML, Microsoft Excel usw.). Anwendungen können die Dateien direkt lesen und beschreiben, da der Schutz der Dateien transparent erfolgt. Benutzer mit Zugriff auf den freigegebenen Speicherplatz können die Dateien zwar sehen, sie jedoch nicht verwenden oder lesen.

PGP NetShare ist eine reine Clientsoftware. Es muss also nichts auf dem Dateiserver installiert werden und die Anwendung funktioniert mit Ihrer vorhandenen Speicherinfrastruktur. Die Verschlüsselung und Entschlüsselung der geschützten Dateien und Ordner erfolgt ausschließlich auf dem Client. Bei Server-Sicherheitskopien werden die verschlüsselten Dateien (Ciphertext) archiviert und können ohne Leseberechtigung nicht gelesen werden.

Personen mit Zugriff auf die geschützten Dateien werden als *Benutzer* bezeichnet. Ordner, in denen sich geschützte Dateien befinden, werden als *geschützte Ordner* bezeichnet.

Benutzern werden Rollen zugewiesen, die die für den Benutzer zugänglichen Aktionen definieren. Weitere Informationen zu Rollen finden Sie unter *PGP NetShare-Rollen* (auf Seite 252).

Ein geschützter Ordner ist ein beliebiger Ordner, der für das Speichern von geschützten Dateien bestimmt ist. Wenn Sie einen Ordner in einen geschützten Ordner konvertieren, werden die enthaltenen Dateien automatisch verschlüsselt. Nach der Erstellung des geschützten Ordners hinzugefügte Dateien werden ebenfalls automatisch verschlüsselt. Sie können einzelne Dateien auch schützen, indem Sie auf **Extras > PGP-Optionen** klicken und auf der Registerkarte „NetShare“ die Option **Einzelne Dateien schützen auswählen.**

Achtung: PGP NetShare bietet *keine* Zugriffssteuerung für die Dateien in einem geschützten Ordner. Da es sich um eine Zugriffssteuerung auf Dateiebene handelt, kann jeder mit Zugriff auf die Dateien in einem geschützten Ordner neue unverschlüsselte Dateien hinzufügen und/oder vorhandene verschlüsselte Dateien entfernen. Daher ist es wichtig, dass Sie den geschützten Ordner an einem sicheren, freigegebenen Speicherort einrichten. Der Netzwerkadministrator kann die Dateien im geschützten Ordner in diesem Fall sichern, ohne sie lesen zu können.

PGP NetShare kann mit den PGP Desktop-Funktionen PGP Virtual Disk und PGP Whole Disk Encryption eingesetzt werden. Sie können also einen geschützten Ordner in PGP Virtual Disk oder bei der Laufwerksverschlüsselung mit PGP Whole Disk Encryption erstellen. Der Schutz mit PGP NetShare ist für Dateien in einer freigegebenen, gemeinsam genutzten Umgebung (in der Regel ein Netzwerk) ausgelegt. PGP Virtual Disk und PGP Whole Disk Encryption schützen einzelne Laufwerke oder Partitionen auf einem lokalen System. Diese drei nützlichen Sicherheitsprodukte sind für geringfügig unterschiedliche Einsatzzwecke konzipiert. Sie können sogar alle drei Produkte auf demselben System verwenden, um Ihre Daten noch sicherer zu schützen.

Das folgende Beispiel soll die Einsatzmöglichkeiten von PGP NetShare veranschaulichen:

Angenommen, Sie sind in einem kleinen Unternehmen mit zwei Hauptproduktlinien für die Finanzen zuständig. Die Unternehmensinhaberin ruft Sie in ihr Büro und bittet Sie, eine Untersuchung zu leiten, ob die Einführung einer weiteren Hauptproduktlinie erfolgreich sein könnte.

Sie möchte, dass Sie mit den Verantwortlichen der Abteilungen Marketing, Verkauf, Entwicklung, Fertigung und Support dieses Thema umfassend erörtern und eine Empfehlung aussprechen. Das gesamte Projekt muss vertraulich behandelt werden.

Glücklicherweise arbeiten alle Benutzer im Unternehmen mit PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung, sodass die Lösung für das Erstellen, Freigeben, Aktualisieren und sichere Speichern von Dateien der Gruppe bereits verfügbar ist: PGP NetShare.

Da die Mitglieder des Projektteams an verschiedenen Standorten arbeiten, müssen Sie für das Projekt einen geschützten Ordner einrichten, der an einem gemeinsamen Speicherort für alle zugänglich ist. Wenn Sie den geschützten Ordner beispielsweise im Firmennetzwerk einrichten, kann jedes Projektmitglied darauf zugreifen.

Nachdem der geschützte Ordner eingerichtet wurde, können die Projektmitglieder neue Dateien hinzufügen, bestehende Dateien öffnen und bearbeiten oder Dateien entfernen, ohne sich Gedanken machen zu müssen, dass diese Dateien durch Verschlüsselung geschützt sind. Verschlüsselung und Entschlüsselung erfolgen vollständig transparent.

Ein weiterer Vorteil von PGP NetShare besteht darin, dass die Dateien für alle unbefugten Benutzer völlig normal aussehen. Der Netzwerkadministrator kann die Dateien im geschützten Ordner daher auf dieselbe Weise sichern wie die anderen Dateien im Netzwerk des Unternehmens. Die Sicherungskopien sind ebenfalls durch Verschlüsselung geschützt.

Hinweis: Die Überwachungs-Engine von PGP NetShare ignoriert mit EFS geschützte Objekte. Dieses Verhalten ist beabsichtigt und stellt sicher, dass Probleme aufgrund der Tatsache vermieden werden, dass EFS eng mit NTFS verbunden ist. Alle Dateien oder Ordner, die mit EFS verschlüsselt sind und in einen durch PGP NetShare geschützten Ordner verschoben oder kopiert werden, behalten die EFS-Verschlüsselung bei, werden jedoch nicht zu durch PGP NetShare geschützten Ordnern. Damit diese Objekte durch PGP NetShare geschützt werden können, müssen Sie die EFS-Verschlüsselung vor dem Kopieren bzw. Verschieben in einen Ordner entfernen.

PGP NetShare bietet für die Dateien in einem geschützten Ordner lückenlose Sicherheit. Die Daten sind immer verschlüsselt, selbst wenn gerade auf einen geschützten Ordner zugegriffen wird oder dieser von einem Projektmitglied an ein anderes Mitglied versendet wird.

Achtung: Wenn Sie für eine geschützte Datei die Option **Speichern unter** auswählen und sie *außerhalb* des geschützten Ordners speichern, ist die neue Version *nicht* geschützt.

PGP NetShare-Rollen

- **Administrator**: Hierbei handelt es sich um den „Besitzer“ des geschützten Ordners. Der Administrator kann Benutzer hinzufügen und entfernen und die Rollen von Benutzern und Gruppenadministratoren ändern. Der Administrator verfügt über vollständigen Lese- und Schreibzugriff auf den geschützten Ordner. Jeder geschützte Ordner kann nur über einen einzigen Administrator verfügen, der automatisch vom Ersteller erstellt wird. Sie müssen einen Administrator für den geschützten Ordner nicht manuell festlegen. Es gibt nur einen Administrator pro Ordner.

  Sie werden ein Administrator, indem Sie einen geschützten Ordner erstellen, sich selbst als Mitglied hinzufügen und sich selbst die Rolle des Administrators zuweisen. Sie können gleichzeitig Mitglied mehrerer Administratorgruppen sein.

  Die Administratorrolle kann von einem Gruppenadministrator nicht entfernt werden, jedoch kann ein Administrator seine Rolle einem anderen Mitglied zuweisen.

  Administratoren müssen über vollständigen Schreibzugriff auf den geschützten Ordner verfügen.

- **Gruppenadministrator**: Hierbei handelt es sich um einen „Administrator“ des geschützten Ordners. Der Gruppenadministrator kann Benutzer hinzufügen und entfernen, Benutzer zu Gruppenadministratoren ernennen oder Gruppenadministratoren in einfache Benutzer ändern. Es kann beliebig viele Gruppenadministratoren geben. Der Gruppenadministrator verfügt über vollständigen Lese- und Schreibzugriff auf den geschützten Ordner. Für jeden durch PGP NetShare geschützten Ordner kann es mehrere Gruppenadministratoren geben.

Gruppenadministratoren müssen über vollständigen Schreibzugriff auf den geschützten Ordner verfügen.

- **Benutzer**: Hierbei handelt es sich um die Benutzer, die berechtigt sind, auf die geschützten Dateien im freigegebenen Speicherplatz zuzugreifen. Die Dateien im geschützten Ordner sind an die Schlüssel der Benutzer verschlüsselt. Sie werden ein Benutzer, wenn ein geschützter Ordner erstellt wird, Sie PGP NetShare hinzugefügt werden und der Administrator oder Gruppenadministrator Ihnen die Rolle eines Benutzers zuweist. Alle Benutzer verfügen über denselben Lese- und Schreibzugriff auf den geschützten Ordner. Benutzer können die Rollen anderer Benutzer nicht ändern. Sie können gleichzeitig Mitglied mehrerer Gruppen von Benutzern sein. Benutzer sind nicht berechtigt, Dateien oder Ordner zu entschlüsseln. Diese Einschränkung besteht, damit Benutzer keine Dateien entschlüsseln und dann mit neuen Rollenzuweisungen wieder verschlüsseln können.

Hinweis: Bei einem Ordner, der mit einer vorherigen Version von PGP Desktop geschützt ist, müssen Sie manuell neue Rollen für vorhandene Benutzer auswählen. Weitere Informationen finden Sie unter *Rollen von Benutzern ändern* (auf Seite 270).

PGP NetShare lizenzieren

Damit Sie PGP NetShare verwenden können, müssen Sie auf dem Computer PGP Desktop 9.5 oder höher ausführen und über eine Lizenz verfügen, die PGP NetShare unterstützt.

So ermitteln Sie, ob Ihre Kopie von PGP Desktop die Komponente PGP NetShare unterstützt

1. Öffnen Sie PGP Desktop.
2. Wählen Sie **Hilfe > Lizenz** aus. Das Dialogfeld für die PGP Desktop-Lizenz wird angezeigt.
3. Im Bereich **Produktinformationen** ist das Symbol **PGP NetShare** aufgeführt. Zeigen Sie mit der Maus auf den Produktnamen, um Informationen zum Produkt anzuzeigen und zu erfahren, ob Sie derzeit über eine gültige Nutzungslizenz verfügen. Wird PGP NetShare nicht unterstützt, wenden Sie sich an den PGP-Administrator, um sich über den Erhalt einer Lizenz für PGP NetShare zu erkundigen.

Wenn Sie mit einer inzwischen abgelaufenen Lizenz von PGP NetShare einen oder mehrere geschützte Ordner erstellt haben, können Sie keine weiteren geschützten Ordner mehr erstellen. Darüber hinaus können Sie die derzeit in den geschützten Ordnern enthaltenen Dateien nicht mehr verwenden, keine Dateien in bestehende geschützte Ordner einfügen und auch nicht mehr als autorisierter Benutzer für einen neuen geschützten Ordner hinzugefügt werden.

Wenn Sie wieder Zugriff auf die verschlüsselten Dateien in einem vorhandenen geschützten Ordner erhalten möchten, benötigen Sie entweder eine neue PGP NetShare-Lizenz oder müssen die Dateien bzw. Ordner im geschützten Ordner entschlüsseln, indem Sie den Befehl **<Dateiname> aus PGP NetShare entfernen** verwenden (weitere Informationen finden Sie unter *Mithilfe des Kontextmenüs auf PGP NetShare-Funktionen zugreifen* (auf Seite 280)).

Schlüssel autorisierter Benutzer

PGP NetShare nutzt die PGP-Schlüssel der von Ihnen angegebenen Benutzer, um den Zugriff auf die entschlüsselten Dateien im geschützten Ordner zu steuern. Die privaten Schlüssel der autorisierten Benutzer werden verwendet, um neue Dateien zu signieren, die dem geschützten Ordner hinzugefügt werden.

Hinweis: PGP NetShare unterstützt nicht die Verwendung von Passphrasen zum Schützen von Dateien. Hierfür müssen PGP-Schlüssel verwendet werden.

Wenn eine Benutzergruppe erstellt wird, legt der Ersteller die öffentlichen Schlüssel der Benutzer fest, die die Dateien im geschützten Ordner nutzen können. Damit die Benutzer diese Dateien verwenden können, müssen sie auf ihrem System über den entsprechenden privaten Schlüssel verfügen, um auf die entschlüsselten Dateien zugreifen zu können.

PGP NetShare-Administratoren (Besitzer) einrichten

Obwohl ein PGP NetShare-Administrator für einen geschützten Ordner nicht erforderlich ist, sollten Sie dennoch in Betracht ziehen, einen der autorisierten Benutzer oder Gruppenadministratoren für diese Rolle auszuwählen. Diese Person wäre dafür verantwortlich, die Dateien und Ordner im geschützten Ordner zu überwachen und Benutzer und Gruppenadministratoren hinzuzufügen und zu entfernen. Zudem müsste sie sicherstellen, dass der geschützte Ordner wie vorgesehen genutzt wird.

Da alle autorisierten Benutzer Dateien, Ordner und (in bestimmten Fällen) Benutzer hinzufügen und entfernen können, werden im Laufe der Zeit möglicherweise Dateien dem geschützten Ordner nicht ordnungsgemäß hinzugefügt bzw. daraus entfernt. Ähnliches kann auch auf das Hinzufügen oder Entfernen von Benutzern zutreffen.

Der Administrator eines geschützten Ordners überwacht die Benutzer und den geschützten Ordner im Hinblick auf diese Probleme und greift bei Bedarf korrigierend ein.

Negativ gelistete und positiv gelistete Dateien, Ordner und Anwendungen

Bestimmte Dateien, Ordner und Anwendungen können negativ gelistet oder positiv gelistet sein. Negativ oder positiv gelistete Objekte werden entweder immer oder niemals geschützt.

Negativ gelistete und andere Dateien, die nicht geschützt werden können

Bestimmte Dateien und Ordner können nicht durch PGP NetShare geschützt werden. Bevor eine Datei oder ein Ordner von PGP NetShare geschützt wird, erfolgt eine Prüfung anhand der so genannten „Negativliste". Ist eine Datei oder ein Ordner negativ gelistet, setzt PGP NetShare die Erstellung des geschützten Ordners fort, die betreffende Datei bzw. der Ordner wird jedoch übersprungen und in der Fortschrittsanzeige des PGP NetShare-Assistenten wird die Meldung angezeigt, dass die Datei bzw. der Ordner negativ gelistet ist.

Zu den negativ gelisteten Dateien zählen u. a. folgende:

- Alle Dateien mit den Dateiendungen `*.skr`, `*.pkr` und `*.pgd`. Dadurch wird verhindert, dass Sie Ihre Schlüssel oder PGP Virtual Disk-Laufwerke verschlüsseln.
- Der Installationsordner von PGP Desktop sowie alle darin enthaltenen Dateien (standardmäßig ist dies der Ordner `C:\Programme\PGP Corporation\PGP Desktop`).
- Der Ordner mit den PGP-Einstellungen sowie alle darin enthaltenen Dateien (standardmäßig ist dies der Ordner `C:\Dokumente und Einstellungen\[Ihr Benutzername]\Anwendungsdaten\PGP Corporation\PGP`).
- Der Ordner für den PGP-Standardschlüsselbund (standardmäßig befindet sich der Schlüsselbund im Ordner „Eigene Dateien").

Darüber hinaus ist es nicht möglich, Dateien und Ordner mit festgelegtem Systemattribut, Dateien und Ordner aus dem Windows-Installationsverzeichnis (standardmäßig sind dies die Ordner `C:\Windows` und `C:\Windows\System32`) oder die Datei `Thumbs.db`, die beim Anzeigen von Miniaturbildern in Windows Explorer erstellt wird, in geschützte Ordner einzufügen. Wenn PGP NetShare Systemdateien oder -ordner hinzugefügt werden, wird die Datei bzw. der Ordner übergangen und im Fortschrittsfenster des PGP NetShare-Assistenten wird eine entsprechende Meldung angezeigt.

Vom PGP Universal Server festgelegte negativ oder positiv gelistete Ordner

Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, hat der PGP-Administrator bestimmte Ordner u. U. negativ oder positiv gelistet.

Negativ gelistete Ordner

Negativ gelistete Ordner sind Ordner, die *nie* zu PGP NetShare hinzugefügt und verschlüsselt werden. Bei negativ gelisteten Ordnern könnte es sich beispielsweise um die Ordner `C:\Programme` oder `C:\Windows\Temp` handeln. Wenn der PGP-Administrator einen Ordner negativ listet, dieser Ordner jedoch nicht vorhanden ist, wird er auch nicht auf dem System erstellt.

Hinweis: Ordner bzw. Dateien, die durch PGP NetShare geschützt wurden, werden nicht automatisch entschlüsselt, wenn sie (durch PGP Universal Server-Richtlinien) negativ gelistet sind. Entfernen Sie den PGP NetShare-Schutz, indem Sie den Ordner bzw. die Datei manuell entschlüsseln. Alle neuen Objekte, die einem geschützten, negativ gelisteten Ordner hinzugefügt werden, erhalten keine PGP NetShare-Verschlüsselung.

Positiv gelistete Ordner

Positiv gelistete Ordner sind Ordner, die *immer* zu PGP NetShare hinzugefügt und verschlüsselt werden. Wenn der PGP-Administrator einen Ordner positiv gelistet hat, dieser Ordner jedoch noch nicht vorhanden ist, wird er auf dem System erstellt. Wenn der PGP-Administrator beispielsweise festlegt, dass der Ordner `C:\Dokumente und Einstellungen\[Benutzername]\Eigene Dateien\Geschützt` auf der Positivliste aufgeführt wird, der Ordner `\Geschützt` jedoch nicht vorhanden ist, wird dieser Ordner erstellt. Auf der Positivliste aufgeführte Ordner können nicht aus PGP NetShare entfernt werden.

Hinweis: Wenn Sie einen Ordner entfernen, der vom PGP Universal-Administrator positiv gelistet wurde, wird dieser Ordner beim nächsten Zugriff auf PGP NetShare oder beim nächsten Starten von PGP Desktop automatisch neu erstellt.

Anwendungsbasierte Verschlüsselungslisten und Umgehungslisten für die Entschlüsselung

Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, hat der PGP Universal Server-Administrator für bestimmte Anwendungen möglicherweise festgelegt, dass mit diesen Anwendungen erstellte Dateien entweder nie entschlüsselt oder immer verschlüsselt werden sollen.

Anwendungsbasierte Verschlüsselungsliste

In dieser Liste sind Anwendungen aufgeführt, in denen alle von der Anwendung geschriebene Dateien verschlüsselt werden müssen. Dateien, die von Anwendungen erstellt werden, die in der anwendungsbasierten Verschlüsselungsliste enthalten sind, werden automatisch an Ihren Schlüssel verschlüsselt und werden immer unabhängig vom Speicherort verschlüsselt (das gilt auch für temporäre Dateien und Systemcaches). Beispiele für Anwendungen, die in dieser Liste enthalten sein können, sind Microsoft Office, Microsoft Excel und Adobe Acrobat.

Andere Verschlüsselungsarten (beispielsweise auf der Positivliste aufgeführte Ordner) haben Vorrang vor Dateien, die von Anwendungen in der anwendungsbasierten Verschlüsselungsliste erstellt wurden.

Der PGP-Administrator könnte z. B. festlegen, dass Microsoft Excel in der anwendungsbasierten Verschlüsselungsliste aufgeführt wird, damit alle von der Finanzabteilung erstellten Arbeitsblätter geschützt sind.

Umgehungslisten für die Entschlüsselung

In dieser Liste sind Anwendungen aufgeführt, in denen alle von der Anwendung geschriebene Dateien nicht automatisch entschlüsselt werden dürfen. Diese Anwendungen werden im Dateiinhalt des Laufwerks bereitgestellt, einschließlich der PGP NetShare-Kopfzeile und dem Ciphertext der Datei. Anwendungen in der Umgehungsliste für die Entschlüsselung umgehen effektiv den PGP NetShare-Filter beim Lesen der Datei, sodass die Dateien beim Lesen verschlüsselt bleiben und diese Anwendungen die verschlüsselten Daten an andere Anwendungen weitergeben können. Zu den Anwendungsarten, die in dieser Liste enthalten sein können, zählen beispielsweise Sicherungs- und FTP-Programme.

Andere Verschlüsselungsarten (z. B. negativ gelistete Ordner) haben Vorrang vor Dateien, die von Anwendungen in der Umgehungsliste für die Entschlüsselung erstellt wurden.

Der PGP-Administrator könnte beispielsweise das Sicherungsprogramm für Ihr Unternehmen in die Umgehungsliste für die Entschlüsselung aufnehmen. Alle von dieser Anwendung erstellen Sicherungsdateien sind geschützt und die Verschlüsselung wird beibehalten, wenn die Sicherungsdatei an einem anderen Speicherort abgelegt wird.

Mit geschützten Ordnern arbeiten

Ein geschützter Ordner ist ein beliebiger Ordner, der für das Speichern von geschützten Dateien bestimmt ist. Wenn Sie einen Ordner in einen geschützten Ordner konvertieren, werden die enthaltenen Dateien automatisch verschlüsselt. Nach der Erstellung des geschützten Ordners hinzugefügte Dateien werden ebenfalls automatisch verschlüsselt. Sie können einzelne Dateien auch schützen, indem Sie auf **Extras > PGP-Optionen** klicken und auf der Registerkarte „NetShare“ die Option **Einzelne Dateien schützen** auswählen.

Ab PGP NetShare 9.10 können Ordner auf Webservern, die das WebDAV-Protokoll unterstützen (z. B. Microsoft SharePoint), durch PGP NetShare geschützt werden. Beachten Sie, dass bestimmte Dateitypen, z. B. `MHT`-Dateien, erforderlich sind, damit SharePoint ordnungsgemäß funktioniert. Wenn diese Dateitypen auf diese Art verwendet werden, können sie von PGP NetShare nicht verschlüsselt werden. Technische Details zum Schützen von SharePoint-Dateien finden Sie im *PGP Corporation-Wissensdatenbankartikel 1120* (http://support.pgp.com/?faq=1120).

Wenn Sie PGP NetShare mit SharePoint verwenden, müssen Sie für die SharePoint-Website für **Auschecken erfordern** die Option **Nein** auswählen. Dadurch können alle autorisierten Benutzer auf alle vom PGP NetShare-Ordner verwalteten Dateien zugreifen.

Tipp: Stellen Sie sicher, dass eine geeignete Sicherungsstrategie verwendet wird und alle durch PGP NetShare geschützten Ordner regelmäßig gesichert werden.

Speicherort für einen geschützten Ordner auswählen

Die PGP Corporation empfiehlt, einen durch PGP NetShare geschützten Ordner an einem Speicherort einzurichten, der für alle autorisierten Benutzer zugänglich ist. Andere Benutzer sollten jedoch keinen Zugriff erhalten.

Obwohl geschützte Ordner in einem öffentlich zugänglichen Bereich eingerichtet werden können, muss berücksichtigt werden, dass PGP NetShare für die Dateien in einem geschützten Ordner *keine* Zugriffssteuerung übernimmt.

Der Schutzgrad, der mit PGP NetShare erreicht werden kann, hängt davon ab, wie Sie mit den Dateien in einem geschützten Ordner umgehen und wer Zugriff auf die Dateien hat. Berücksichtigen Sie bei der Auswahl des Speicherorts für einen durch PGP NetShare geschützten Ordner folgende Punkte.

- *Normale Verwendung* (auf Seite 259)
- *Dateizugriff* (auf Seite 259)
- *Direkter Zugriff auf verschlüsselte Daten (Ciphertext)* (auf Seite 259)

- *Beschädigte, gelöschte oder überschriebene geschützte Dateien* (auf Seite 260)
- *Negativ gelistete und andere Dateien, die nicht geschützt werden können* (auf Seite 255)

Normale Verwendung

Bei der normalen Verwendung durch einen autorisierten Benutzer werden die Dateien in einem geschützten Ordner durch PGP NetShare vollständig geschützt. Normale Verwendung bedeutet in diesem Zusammenhang, dass eine geschützte Datei geöffnet, bearbeitet und gespeichert wird, dass eine neue Datei in einem geschützten Ordner erstellt wird oder dass eine Datei in einen geschützten Ordner verschoben oder kopiert wird.

Wenn eine Datei aus einem durch PGP NetShare geschützten Ordner verschoben oder kopiert wird, versucht PGP NetShare, die Datei geschützt zu halten. Dadurch können Sie Dateien beispielsweise aus einem geschützten Ordner auf ein USB-Laufwerk kopieren, ohne den Dateischutz zu verlieren. Wenn Sie eine Datei aus einem geschützten Ordner verschieben oder kopieren, sollten Sie sich vergewissern, dass die Zieldatei weiterhin geschützt ist. Beachten Sie hierzu das Schlosssymbol oder zeigen Sie die Dateieigenschaften an.

Dateizugriff

Alle von Ihnen verwendeten Anwendungen können uneingeschränkt auf die entschlüsselten Daten der durch PGP NetShare geschützten Dateien zugreifen. Dies umfasst andere Anwendungen der PGP Corporation, z. B. PGP Zip. Wenn Sie also ein PGP Zip-Archiv erstellen und eine durch PGP NetShare geschützte Datei einfügen, enthält das PGP Zip-Archiv eine entschlüsselte Version der Datei.

Wenn Sie für eine geschützte Datei die Option **Speichern unter** auswählen und sie *außerhalb* des geschützten Ordners speichern, müssen Sie zudem beachten, dass die neue Version *nicht* geschützt ist.

Direkter Zugriff auf verschlüsselte Daten (Ciphertext)

Unter bestimmten Bedingungen kann PGP NetShare umgangen werden, sodass direkt auf die verschlüsselten Daten bzw. den Ciphertext der verschlüsselten Datei zugegriffen werden kann.

Auf diese Weise kann ein Benutzer (z. B. der Netzwerkadministrator) der zwar physischen Zugriff auf die geschützten Dateien hat, jedoch nicht mit PGP Desktop arbeitet, die geschützten Dateien auf einem Dateiserver sichern, verschieben, kopieren, per FTP übertragen usw. In diesen Fällen würde der Ciphertext der geschützten Dateien gesichert, verschoben, kopiert bzw. per FTP übertragen werden.

Beschädigte, gelöschte oder überschriebene geschützte Dateien

PGP NetShare bietet *keine* Zugriffssteuerung für Dateien. Obwohl Benutzer ohne befugten Zugriff Dateien in geschützten Ordnern nicht öffnen können, haben sie dennoch Zugriff auf diese Dateien. Das bedeutet, dass der Dateischutz von PGP NetShare keine Sicherheit gegen Beschädigung, Löschen oder Überschreiben von Dateien durch Benutzer darstellt, die Zugriff auf diese Dateien haben. PGP NetShare schützt den Inhalt einer Datei, jedoch nicht die Datei selbst.

Daher wird dringend empfohlen, zusätzlich zur kryptografischen Zugriffskontrolle und zu dem von PGP NetShare gebotenen Schutz weitere wirksame Maßnahmen für die Dateizugriffskontrolle einzusetzen.

Neue durch PGP NetShare geschützte Ordner erstellen

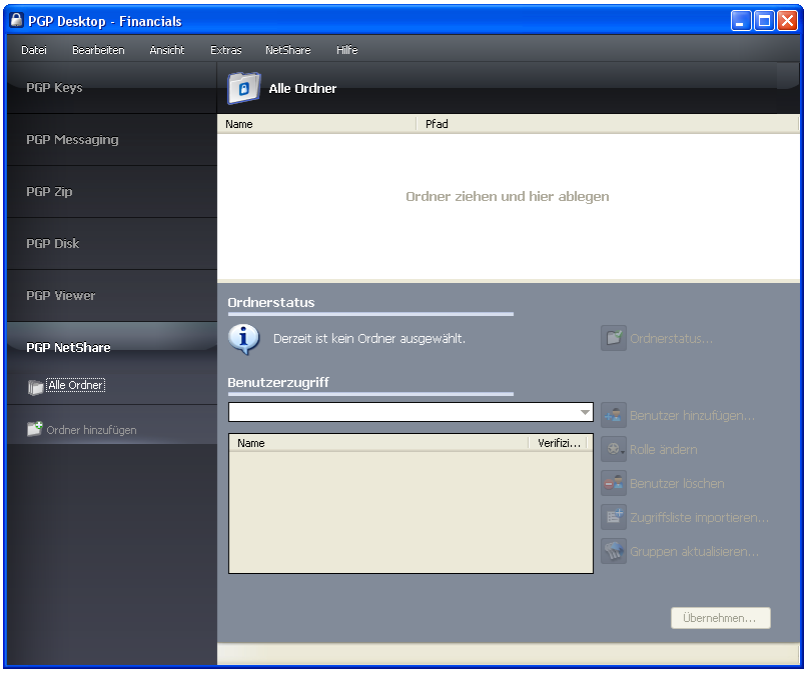
Der geschützte Ordner enthält alle durch PGP NetShare geschützte Dateien.

Tipp: Beim Erstellen eines neuen durch PGP NetShare geschützten Ordners wird das Änderungsdatum der bereits im Ordner vorhandenen Dateien in das Datum des PGP NetShare-Vorgangs geändert. Wenn das Änderungsdatum nicht angepasst werden soll, erstellen Sie *zuerst* einen leeren PGP NetShare-Ordner und fügen Sie diesem Ordner *dann* Dateien hinzu.

Hinweis: Sie müssen über Schreibberechtigungen verfügen, um einen durch PGP NetShare geschützten Ordner erstellen zu können.

So erstellen Sie einen neuen durch PGP NetShare geschützten Ordner

1 Öffnen Sie PGP Desktop und klicken Sie auf das Bedienfeld für PGP NetShare. Der PGP NetShare-Arbeitsbereich wird angezeigt.



2 Führen Sie einen der folgenden Schritte aus:

- Ziehen Sie den Ordner, den Sie als geschützten Ordner vorgesehen haben, in das Feld mit der Beschriftung „Ordner ziehen und hier ablegen“. Dadurch wird der PGP NetShare-Assistent geöffnet und der Schritt zum Festlegen des geschützten Ordners übersprungen.
- Klicken Sie im Bedienfeld für PGP NetShare auf **Ordner hinzufügen** oder wählen Sie **NetShare > Ordner hinzufügen** aus. Im PGP NetShare-Assistenten wird der Bildschirm „Ordner auswählen“ angezeigt.
  - Klicken Sie auf **Durchsuchen**. Das Dialogfeld „Ordner suchen“ wird angezeigt.
  - Wechseln Sie zu dem Ordner mit den Dateien, die im geschützten Ordner abgelegt werden sollen. Wenn Sie einen leeren Ordner erstellen möchten, um dort die Dateien für den geschützten Ordner abzulegen, klicken Sie auf **Neuen Ordner erstellen**.
  - Klicken Sie auf **OK**, um das Dialogfeld **Ordner suchen** zu schließen. Der Bildschirm **Ordner auswählen** wird erneut angezeigt.
- (Optional) Geben Sie in das Feld **Beschreibung** eine Beschreibung für den geschützten Ordner ein.

3 Klicken Sie auf **Weiter**. Der Bildschirm „Benutzer hinzufügen“ wird angezeigt.

4 Wenn Sie Benutzer für den geschützten Ordner, den Sie erstellen, hinzufügen möchten, klicken Sie auf das Symbol mit dem Pfeil nach unten. Eine Liste der Schlüssel am Schlüsselbund wird angezeigt.

5 Wählen Sie einen Benutzer aus und klicken Sie auf **Hinzufügen**.

Hinweis: Wenn Sie selbst auf den Inhalt des geschützten Ordners zugreifen möchten, müssen Sie Ihren eigenen Schlüssel hinzufügen. Andernfalls können Sie die Dateien im geschützten Ordner nicht verwenden.

Sie können autorisierte Benutzer auch hinzufügen, indem Sie auf **Hinzufügen** klicken. Das Dialogfeld „Benutzerauswahl“ wird angezeigt.

6 Führen Sie einen der folgenden Schritte aus:

- Ziehen Sie Schlüssel aus der Spalte **Schlüsselquelle** in die Spalte **Hinzuzufügende Schlüssel**.
- Klicken Sie in der Spalte **Schlüsselquelle** auf einen Schlüssel und dann auf **Hinzufügen**.
- Doppelklicken Sie in der Spalte **Schlüsselquelle** auf einen Schlüssel.
- Fügen Sie Schlüssel aus dem PGP Global Directory hinzu, indem Sie auf das Symbol von PGP Global Directory klicken, einen Suchbegriff in das Feld **Suchen** eingeben und zum Starten der Suche auf die Lupe klicken. Das Suchergebnis wird in der Spalte **Schlüsselquelle** angezeigt. Fügen Sie die Schlüssel aus dieser Spalte in die Spalte **Hinzuzufügende Schlüssel** ein.

Hinweis: PGP NetShare weist neu hinzugefügte Mitglieder nicht automatisch darauf hin, dass sie einem geschützten Ordner als autorisierte Benutzer hinzugefügt wurden. Grundsätzlich unterliegt es der Verantwortung des Erstellers des neuen geschützten Ordners, die Mitglieder darüber zu informieren, dass der geschützte Ordner erstellt wurde und dass sie autorisierte Benutzer sind.

7 Klicken Sie auf **OK**, um den Bildschirm „Benutzerauswahl“ zu schließen. Der Bildschirm **Benutzer hinzufügen** wird erneut angezeigt.

8 Weisen Sie den einzelnen Benutzern Rollen zu, indem Sie mit der rechten Maustaste auf den jeweiligen Benutzernamen klicken und eine Rolle auswählen:

- **Administrator**: Erstellen Sie nur einen Administrator pro geschütztem PGP NetShare-Ordner. Diese Rolle verfügt über vollständigen Lese-/Schreibzugriff auf den Ordner, kann Benutzer hinzufügen und entfernen, anderen Benutzern Rollen zuweisen sowie andere Benutzer als Administratoren einrichten.

- **Gruppenadministrator**: Erstellen Sie für jeden geschützten PGP NetShare-Ordner beliebig viele Gruppenadministratoren. Diese Rolle verfügt über vollständigen Lese-/Schreibzugriff auf den Ordner, kann Benutzer hinzufügen und entfernen sowie anderen Benutzern Rollen zuweisen.
- **Benutzer**: Erstellen Sie für jeden geschützten PGP NetShare-Ordner beliebig viele Benutzer. Diese Rolle verfügt über vollständigen Lese-/Schreibzugriff auf den Ordner.

Sie können die Rolle eines Benutzers jederzeit nach der Erstellung des geschützten Ordners ändern. Klicken Sie in PGP Desktop auf den geschützten Ordner und anschließend mit der rechten Maustaste auf den Benutzernamen, um die Rolle dieses Benutzers zu ändern.

9 Klicken Sie auf **Weiter**. Der Bildschirm „Signierer auswählen“ wird angezeigt.

10 Wählen Sie aus den privaten Schlüsseln am lokalen Schlüsselbund einen privaten Schlüssel aus. Dieser Schlüssel dient zum Signieren der Dateien, die durch Verschlüsselung im geschützten Ordner geschützt werden.

11 Geben Sie die **Passphrase** für den Schlüssel ein.

12 Klicken Sie auf **Weiter**. Die Fortschrittsanzeige wird angezeigt.

Die Dateien im geschützten Ordner werden verschlüsselt und die angegebenen Benutzer werden als autorisierte Benutzer hinzugefügt.

Hinweis: Wenn Sie den Verschlüsselungsvorgang abbrechen, bleiben bereits verschlüsselte Dateien verschlüsselt. Informationen zum Wiederherstellen des ursprünglichen unverschlüsselten Zustands der Dateien finden Sie unter *Ordner entfernen* (siehe "Durch PGP NetShare geschützte Ordner entschlüsseln" auf Seite 275).

13 Klicken Sie nach Abschluss des Vorgangs auf **Fertig stellen**.

Dateien in durch PGP NetShare geschützten Ordnern verwenden

Als autorisierter PGP NetShare-Benutzer haben Sie drei Möglichkeiten, auf die Dateien im geschützten Ordner zuzugreifen:

- Doppelklicken Sie auf den geschützten Ordner, um ihn zu öffnen, und doppelklicken Sie dann auf die gewünschte Datei.
- Öffnen Sie die gewünschte Datei in der Anwendung, in der die Datei erstellt wurde.
- Öffnen Sie den geschützten Ordner, indem Sie auf den Hypertext-Link des dazugehörigen Pfades klicken, und doppelklicken Sie dann auf die gewünschte Datei.

Wenn die Passphrase des privaten Schlüssels, der für Ihre Mitgliedschaft im durch PGP NetShare geschützten Ordner verwendet wird, auf dem System zwischengespeichert wurde, werden die Dateien automatisch geöffnet. Sie müssen daher zum Öffnen der Dateien keine weiteren Schritte durchführen.

Falls die Passphrase nicht zwischengespeichert wurde, ist der geschützte Ordner jedoch gesperrt. Sie müssen sich authentifizieren, bevor Sie die Dateien im geschützten Ordner öffnen können. Weitere Informationen finden Sie unter *Geschützte Ordner entsperren* (auf Seite 264).

Hinweis: Wenn Sie unter Windows Vista ein durch PGP NetShare geschütztes Textdokument in Editor öffnen, werden zwei Benachrichtigen angezeigt, dass die Datei entsperrt wird. Dies liegt in der Art und Weise begründet, auf die Editor auf die Datei zugreift.

Geschützte Ordner entsperren

Mit der Schaltfläche **Entsperren** können Sie versuchen, auf einen scheinbar gesperrten Ordner zuzugreifen und ihn zu entsperren. Sie können den Befehl auch in Situationen nutzen, in denen ein Ordner manuell entsperrt werden muss. Ein geschützter Ordner muss manuell entsperrt werden, wenn er aus einem der folgenden Gründe gesperrt ist:

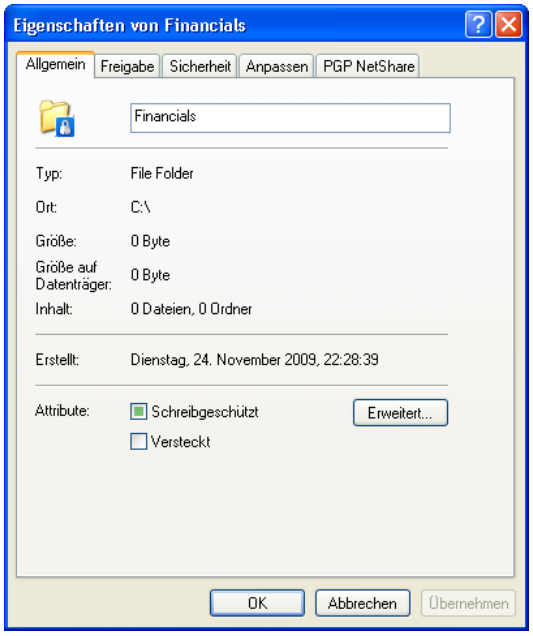
- Bei der Eingabe der Passphrase ist eine Zeitüberschreitung aufgetreten.
- Sie klicken im Passphrasendialogfeld auf **Abbrechen**, ohne eine gültige Passphrase einzugeben.

Alle zukünftigen Versuche, auf den geschützten Ordner zuzugreifen, werden durch das Dialogfeld „Der Zugriff wurde verweigert“ abgewiesen und Sie müssen jeden Ordner entsperren, bevor Sie dessen Dateien verwenden können.

So entsperren Sie einen geschützten Ordner

1 Klicken Sie mit der rechten Maustaste auf den geschützten Ordner und wählen Sie **PGP Desktop > PGP NetShare-Eigenschaften** aus.

2 Die Registerkarte mit den PGP NetShare-Eigenschaften wird angezeigt.



3 Klicken Sie auf **Entsperren**. Das Dialogfeld **Entsperren** wird angezeigt.

4 Geben Sie die entsprechende Passphrase ein und klicken Sie auf **OK**. Das Dialogfeld „Entsperren“ wird geschlossen. Die Passphrase wird zwischengespeichert und Sie erhalten Zugriff auf alle Dateien im geschützten Ordner.

Hinweis: Falls der PGP Universal Server-Administrator diese Option aktiviert hat, können Sie im Menü des PGP-Symbols im Infobereich der Taskleiste die Option **NetShare-Sperren erneut durchsuchen** auswählen. Verwenden Sie diese Option, um einen durch PGP NetShare geschützten Ordner zu entsperren, wenn sich der Schlüssel auf einer Smartcard oder einem Token befindet, die bzw. der beim Zugriff auf den Ordner nicht eingesteckt war.

Dateien in einem geschützten Ordner ermitteln

Als autorisierter Benutzer haben Sie uneingeschränkten Zugriff auf alle Dateien im geschützten Ordner. Wenn Sie den geschützten Ordner selbst erstellt haben, ist Ihnen der Inhalt des Ordners wahrscheinlich bekannt. Wenn Sie dem geschützten Ordner jedoch von einem anderen Mitglied hinzugefügt wurden, wissen Sie möglicherweise nicht sofort, welche Dateien im geschützten Ordner zur Verfügung stehen.

So ermitteln Sie, welche Dateien sich in einem geschützten Ordner befinden

1 Öffnen Sie PGP Desktop und klicken Sie auf das Bedienfeld für PGP NetShare.

2 Klicken Sie auf den als Hyperlink angezeigten Pfad zum geschützten Ordner. Der Inhalt des geschützten Ordners wird in einem neuen Fenster angezeigt, das alle Dateien und Ordner enthält, die sich im geschützten Ordner befinden.

Wenn der Zugriff verweigert wird, ist der geschützte Ordner gesperrt. Öffnen Sie in diesem Fall entweder im Eigenschaftenfenster des gesperrten Ordners die Registerkarte „PGP NetShare“ und heben die Ordnersperre auf oder starten Sie das System neu, um Zugriff zu erhalten. Weitere Informationen zum Entsperren von geschützten Ordnern finden Sie unter *Dateien in durch PGP NetShare geschützten Ordnern verwenden* (auf Seite 263).

Unterordner zu geschützten Ordnern hinzufügen

PGP NetShare unterstützt sowohl das Hinzufügen von Dateien als auch von Ordnern zu einem geschützten Ordner, nachdem dieser erstellt wurde.

Alle Dateien eines Ordners, den Sie einem geschützten Ordner hinzufügen, werden automatisch geschützt. Sowohl der Ordner als auch die Dateien stehen dann nur autorisierten Benutzern zur Verfügung.

Fügen Sie dem Ordner keine geschützten Ordner hinzu, die andere autorisierte Benutzer umfassen. Dadurch hätte das neue Unterverzeichnis nicht dieselben autorisierten Benutzer wie der übergeordnete Ordner.

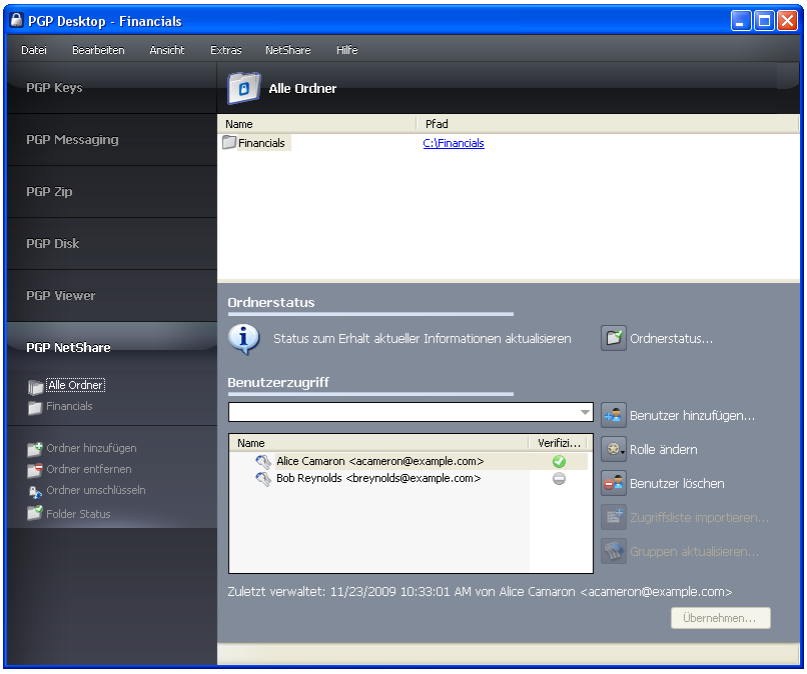
Hinweis: Die Überwachungs-Engine von PGP NetShare ignoriert mit EFS geschützte Objekte. Dieses Verhalten ist beabsichtigt und stellt sicher, dass Probleme aufgrund der Tatsache vermieden werden, dass EFS eng mit NTFS verbunden ist. Alle Dateien oder Ordner, die mit EFS verschlüsselt sind und in einen durch PGP NetShare geschützten Ordner verschoben oder kopiert werden, behalten die EFS-Verschlüsselung bei, werden jedoch nicht zu durch PGP NetShare geschützten Ordnern. Damit diese Objekte durch PGP NetShare geschützt werden können, müssen Sie die EFS-Verschlüsselung vor dem Kopieren bzw. Verschieben in einen Ordner entfernen.

Ordnerstatus prüfen

Mit dem Befehl **Ordnerstatus prüfen** rufen Sie aktuelle Informationen zum Status eines PGP NetShare-Ordners ab. Der Befehl steht im Arbeitsbereich des NetShare-Ordners, im Bedienfeld „PGP NetShare“ und im Menü „NetShare“ zur Verfügung.

So prüfen Sie den Status eines Ordners in einem geschützten Ordner

1 Klicken Sie im Arbeitsbereich von PGP NetShare im Bereich „Ordnerstatus“ auf **Ordnerstatus prüfen**. Es muss ein PGP NetShare-Ordner ausgewählt sein.



2 Links neben der Schaltfläche **Ordnerstatus prüfen** wird der Status des ausgewählten Ordners angezeigt (z. B. „Alle Ordner und Dateien sind verschlüsselt“).

Tipp: Unter der Benutzerliste werden Datum, Uhrzeit und Schlüssel-ID des Benutzers angezeigt, der den geschützten Ordner zuletzt verwaltet hat.

Geschützte Ordner an andere Speicherorte kopieren

Die größtmögliche Sicherheit erhalten Sie, wenn Sie immer in einem geschützten Ordner arbeiten. Die PGP Corporation empfiehlt, beim Kopieren eines Ordners zuerst einen geschützten Ordner als Ziel zu erstellen. Wenn Sie Dateien von einem geschützten Ordner in einen anderen geschützten Ordner kopieren, bleiben die Daten stets geschützt.

PGP NetShare behält die Dateiverschlüsselung bei, selbst wenn der geschützte Ordner an einen anderen Speicherort verschoben wird. Jedoch kann es abhängig vom angewendeten Kopierverfahren oder vom Speicherort dazu kommen, dass der Schutz des *Ordners* verloren geht. Die Dateien im Ordner bleiben geschützt, jedoch können die PGP NetShare-Informationen des Ordners verloren gehen, sodass der Ordner auch nicht mehr mit dem PGP-Symbol angezeigt wird.

Wenn Sie einen Ordner an einen ungeschützten Speicherort kopiert haben, sollten Sie den Ordnerstatus prüfen. Gehen Sie dabei entsprechend der Informationen unter *Ordnerstatus prüfen* (auf Seite 266) vor, um sicherzustellen, dass Ordner und Dateien verschlüsselt werden.

Wenn der Ordner nicht verschlüsselt ist, führen Sie folgende Schritte aus:

1. Wenn Sie über die entsprechenden PGP NetShare-Berechtigungen verfügen, erstellen Sie einen neuen geschützten Ordner als Ziel. Informationen hierzu finden Sie unter *Neue durch PGP NetShare geschützte Ordner erstellen* (auf Seite 260).
2. Kopieren Sie den Inhalt des Ordners, dessen Schutz verloren gegangen ist, in den neuen geschützten Ordner.
3. Importieren Sie die Zugriffsliste des alten Ordners in den neuen Ordner. Informationen hierzu finden Sie unter *PGP NetShare-Zugriffslisten importieren* (auf Seite 272).

Mit PGP NetShare-Benutzern arbeiten

Benutzer mit PGP Desktop 9.5 oder höher, die über ein entsprechendes Schlüsselpaar in PGP Desktop verfügen, können Benutzer eines durch PGP NetShare geschützten Ordners sein.

Dabei kann es verschiedene Schlüsselpaare geben:

- Die Schlüsselpaare wurden in PGP Desktop erstellt.
- Die Schlüsselpaare wurden von einer OpenPGP-Anwendung erstellt und in PGP Desktop importiert.
- Das Schlüsselpaar ist ein X.509-Zertifikat, das in PGP Desktop importiert wurde.

Es gibt zwei Möglichkeiten, ein Benutzer zu werden:

- Sie können mit PGP Desktop einen geschützten Ordner erstellen und sich selbst als Benutzer hinzufügen.
- Sie können von einem vorhandenen Mitglied als Benutzer hinzugefügt werden.

Sobald Sie ein Benutzer sind, haben Sie dieselben Rechte wie alle anderen Benutzer.

PGP NetShare-Benutzer hinzufügen

Die meisten PGP NetShare-Benutzer werden beim Erstellen eines geschützten Ordners hinzugefügt. Sie können jedoch auch jederzeit später Mitglieder hinzufügen, sofern Sie ein Administrator oder ein Gruppenadministrator des geschützten Ordners sind.

Achtung: Wählen Sie die Benutzer von PGP NetShare mit Sorgfalt aus. Sobald eine Person als Benutzer hinzugefügt wurde, verfügt sie über die gleichen Rechte wie alle anderen Benutzer. Das neue Mitglied kann dem geschützten Ordner neue Dateien hinzufügen oder vorhandene Dateien aus diesem Ordner entfernen.

So fügen Sie einen neuen PGP NetShare-Benutzer hinzu

1. Wählen Sie den PGP NetShare-Ordner aus, dem Sie ein neues Mitglied hinzufügen möchten.
2. Klicken Sie im Bereich „Benutzerzugriff“ auf **Benutzer hinzufügen**. Das Dialogfeld „Benutzerauswahl“ wird angezeigt.
3. Führen Sie einen der folgenden Schritte aus:
   - Ziehen Sie Schlüssel aus der Spalte **Schlüsselquelle** in die Spalte **Hinzuzufügende Schlüssel**.
   - Klicken Sie in der Spalte **Schlüsselquelle** auf einen Schlüssel und dann auf **Hinzufügen**.
   - Fügen Sie Schlüssel aus dem PGP Global Directory hinzu, indem Sie auf das Symbol von PGP Global Directory klicken, einen Suchbegriff in das Feld **Suchen** eingeben und zum Starten der Suche auf die Lupe klicken bzw. die **Eingabetaste** drücken. Das Suchergebnis wird in der Spalte **Schlüsselquelle** angezeigt. Fügen Sie die Schlüssel aus dieser Spalte in die Spalte **Hinzuzufügende Schlüssel** ein.

   Hinweis: PGP NetShare weist neu hinzugefügte Mitglieder nicht darauf hin, dass sie als autorisierte Benutzer hinzugefügt wurden. Grundsätzlich liegt es in der Verantwortung der Person, die neue Benutzer hinzugefügt hat, die betroffenen Personen zu informieren, dass sie autorisierte Benutzer sind.
4. Klicken Sie auf **OK**. Der Benutzer wird der Benutzerliste hinzugefügt.
5. Klicken Sie auf **Übernehmen**. Der Bildschirm „Signierer auswählen“ wird angezeigt.

6 Wählen Sie aus den privaten Schlüsseln am lokalen Schlüsselbund einen Schlüssel aus oder akzeptieren Sie den Standardschlüssel. Dieser Schlüssel dient bei der Umschlüsselung zum Signieren der Dateien. Wenn Benutzer hinzugefügt werden, erfolgt als Sicherheitsmaßnahme automatisch eine Umschlüsselung der Dateien im geschützten Ordner.

7 Geben Sie die Passphrase für den ausgewählten Schlüssel ein, sofern sie nicht zwischengespeichert ist, und klicken Sie auf **Weiter**. Die Fortschrittsanzeige wird angezeigt und die Dateien im angegebenen geschützten Ordner werden umgeschlüsselt.

8 Klicken Sie auf **Beenden**.

Rollen von Benutzern ändern

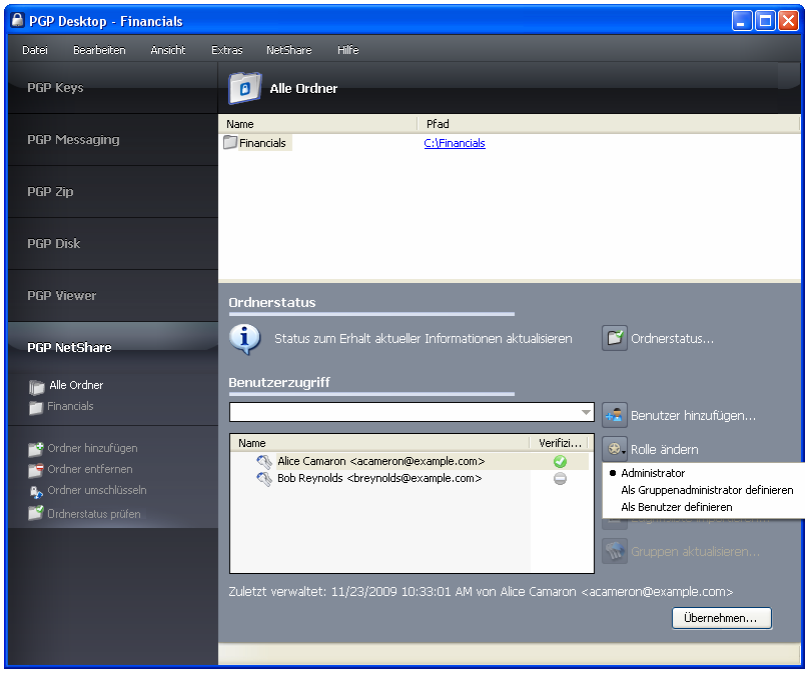
Sie können die Rolle eines Benutzers jederzeit nach der Erstellung des geschützten Ordners ändern. Weitere Informationen zu Rollen finden Sie unter *PGP NetShare-Rollen* (auf Seite 252).

Wenn Sie einen Benutzer in einen Administrator oder in einen Gruppenadministrator ändern möchten, müssen Sie sicherstellen, dass der Benutzer über sämtliche Berechtigungen für den geschützten Ordner verfügt.

So ändern Sie die Rolle eines Benutzers

1 Wählen Sie in PGP Desktop den PGP NetShare-Ordner aus, dem Sie ein neues Mitglied hinzufügen möchten.

2 Klicken Sie im Bereich „Benutzerzugriff“ auf den Benutzernamen und dann auf **Rolle ändern**.



Tipp: Sie können auch mit der rechten Maustaste auf den Benutzernamen klicken und die Rolle auswählen.

3 Wählen Sie in der angezeigten Liste die Rolle aus, die für diesen Benutzer gelten soll:

- **Administrator**: Erstellen Sie nur einen Administrator pro geschütztem PGP NetShare-Ordner. Diese Rolle verfügt über vollständigen Lese-/Schreibzugriff auf den Ordner, kann Benutzer hinzufügen und entfernen, anderen Benutzern Rollen zuweisen sowie andere Benutzer als Administratoren einrichten.
- **Gruppenadministrator**: Erstellen Sie für jeden geschützten PGP NetShare-Ordner beliebig viele Gruppenadministratoren. Diese Rolle verfügt über vollständigen Lese-/Schreibzugriff auf den Ordner, kann Benutzer hinzufügen und entfernen sowie anderen Benutzern Rollen zuweisen.
- **Benutzer**: Erstellen Sie für jeden geschützten PGP NetShare-Ordner beliebig viele Benutzer. Diese Rolle verfügt über vollständigen Lese-/Schreibzugriff auf den Ordner.

4 Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern.

Benutzer aus geschützten Ordnern löschen

Wenn Sie ein Mitglied eines durch PGP NetShare geschützten Ordners entfernen möchten, müssen Sie den betreffenden Benutzer löschen.

So löschen Sie einen Benutzer aus einem durch PGP NetShare geschützten Ordner

1. Wählen Sie im Bildschirm „PGP NetShare“ den geschützten Ordner, aus dem Sie den Benutzer löschen möchten.
2. Klicken Sie in der Liste „Benutzerzugriff“ unten im Bildschirm auf den Namen des Benutzers, den Sie löschen möchten, und dann auf die Schaltfläche **Benutzer löschen**. Der ausgewählte Benutzer wird aus der Liste gelöscht.
3. Klicken Sie auf **Übernehmen**. Der Bildschirm „Signierer auswählen“ wird angezeigt.
4. Wählen Sie aus den privaten Schlüsseln am lokalen Schlüsselbund einen Schlüssel aus oder akzeptieren Sie den Standardschlüssel. Dieser Schlüssel dient bei der Umschlüsselung zum Signieren der Dateien. Wenn ein Mitglied aus einem geschützten Ordner entfernt wird, werden die Dateien in diesem Ordner als Sicherheitsmaßnahme automatisch umgeschlüsselt.
5. Geben Sie nach der entsprechenden Aufforderung die Passphrase für den ausgewählten Schlüssel ein und klicken Sie auf **Weiter**. Die Fortschrittsanzeige wird angezeigt und die Dateien im angegebenen geschützten Ordner werden umgeschlüsselt.
6. Klicken Sie auf **Beenden**. Der gelöschte Benutzer wurde als Mitglied des geschützten Ordners entfernt und kann nicht mehr auf die Dateien in diesem Ordner zugreifen.

PGP NetShare-Zugriffslisten importieren

Beim Importieren von Zugriffslisten importieren Sie die Mitglieder und deren Schlüssel aus einer Gruppe autorisierter Benutzer, der Sie angehören, in eine andere Gruppe autorisierter Benutzer, der Sie ebenfalls angehören.

Diese Option ist nur verfügbar, wenn Sie über mehrere geschützte Ordner verfügen.

So importieren Sie eine Zugriffsliste

1. Wählen Sie im Bildschirm „PGP NetShare“ den geschützten Ordner aus, in den Sie die Mitglieder eines anderen geschützten Ordners importieren möchten.

2 Klicken Sie in der Liste **Benutzerzugriff** unten im Bildschirm auf **Zugriffsliste importieren**. Das Dialogfeld „PGP-Benutzerzugriffsliste importieren“ wird angezeigt.

3 Klicken Sie auf den Namen des vorhandenen geschützten Ordners, dessen Mitglieder Sie importieren möchten, und klicken Sie auf **Importieren**.

4 Klicken Sie auf **Übernehmen**. Das Dialogfeld „Signierer auswählen“ wird angezeigt.

5 Wählen Sie aus den privaten Schlüsseln am lokalen Schlüsselbund einen Schlüssel aus oder akzeptieren Sie den Standardschlüssel. Dieser Schlüssel dient bei der Umschlüsselung zum Signieren der Dateien. Wenn die Mitglieder eines Ordners geändert werden, erfolgt als Sicherheitsmaßnahme automatisch eine Umschlüsselung der Dateien im geschützten Ordner.

6 Geben Sie nach der entsprechenden Aufforderung die Passphrase für den ausgewählten Schlüssel ein und klicken Sie auf **Weiter**. Die Fortschrittsanzeige wird angezeigt und die Dateien im angegebenen geschützten Ordner werden umgeschlüsselt.

7 Klicken Sie auf **Beenden**. Die neuen Mitglieder werden dem geschützten Ordner hinzugefügt.

Mit Active Directory-Gruppen arbeiten

PGP NetShare kann mit Active Directory integriert werden, sodass Sie Benutzer problemlos den geschützten Ordnern einer Active Directory-Gruppe zuweisen können. PGP NetShare verwendet LDAP (Lightweight Directory Access Protocol), um Gruppeninformationen aus dem Active Directory Ihrer Organisation abzurufen.

PGP NetShare für die Arbeit mit Gruppen einrichten

Damit Sie Gruppeninformationen abrufen können, müssen Sie eine Bindung mit dem PGP Universal Server herstellen und dann die Option **Für Gruppenerweiterung verwenden** aktivieren. In der folgenden Anleitung werden die Schritte bei einer Installation von PGP Desktop als eigenständige Anwendung beschrieben. Wenn PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung installiert ist und eingesetzt wird, müssen Sie diese Schritte nicht ausführen, da die LDAP-Integration automatisch erfolgt.

Hinweis: Die Anzahl der Benutzer, die gleichzeitig einem PGP NetShare-Ordner hinzugefügt werden können, ist begrenzt (50 Benutzer). Dieser hartcodierte Grenzwert kann zwar angepasst werden, dies hat jedoch gewisse Folgen. Daher sollte ohne die Unterstützung der PGP Corporation kein diesbezüglicher Versuch unternommen werden. Weitere Informationen finden Sie im *PGP-Wissensdatenbankartikel 830* (https://support.pgp.com/?faq=830).

So richten Sie PGP NetShare für die Arbeit mit Gruppen ein

1. Fügen Sie den PGP Universal Server Ihrer Liste bevorzugter Keyserver hinzu. Erstellen Sie hierzu einen neuen Messaging-Dienst und geben Sie den Namen des PGP Universal Servers an. Weitere Informationen finden Sie unter *Dienste erstellen und Kontoeigenschaften bearbeiten* (siehe "Neue Messaging-Dienste erstellen" auf Seite 106).
2. Stellen Sie eine Bindung mit dem PGP Universal Server her. Befolgen Sie hierzu die Anleitungen zum manuellen Binden an einen PGP Universal Server unter *Messaging mit Lotus Notes und MAPI* (siehe "PGP Desktop mit IBM Lotus Notes verwenden" auf Seite 361).
3. Wählen Sie im Assistenten für die Erstellung eines PGP-Schlüssels den Schlüsselmodus „GKM“, „CKM“ oder „SCKM“ aus. Wählen Sie nicht die Option „SKM“ aus.
4. Vergewissern Sie sich, dass der Schlüssel auf dem PGP Universal Server verfügbar ist. Wählen Sie dazu in PGP Desktop das Bedienfeld „PGP Keys“ aus. Klicken Sie auf **Nach Schlüsseln suchen**, wählen Sie den Namen des PGP Universal Servers aus, geben Sie Ihren Namen ein und klicken Sie auf **Suchen**.
5. Aktivieren Sie die Gruppenerweiterung. Wählen Sie dazu in PGP Desktop das Bedienfeld „PGP Messaging“ aus.
6. Klicken Sie auf **Messaging** > **Für Gruppenerweiterung verwenden**. Der Menübefehl wird nun mit einem Häkchen angezeigt und die Option ist aktiviert.

Gruppen aktualisieren

Wenn Sie PGP NetShare in einer von einem PGP Universal Server verwalteten Umgebung einsetzen und der PGP-Administrator Active Directory-Gruppen eingerichtet hat, können Sie mit PGP NetShare verifizieren, ob die Gruppenmitgliedschaften aktuell sind.

So aktualisieren Sie Active Directory-Gruppen

1. Wählen Sie im Bildschirm „PGP NetShare“ den geschützten Ordner aus, dessen Active Directory-Gruppen Sie aktualisieren möchten.

2 Klicken Sie im Bereich **Benutzerzugriff** auf **Gruppen aktualisieren**. PGP NetShare überprüft die Active Directory-Gruppenmitgliedschaften und aktualisiert diese bei Bedarf.

Durch PGP NetShare geschützte Ordner entschlüsseln

Mit dem Befehl „Ordner entfernen“ werden die Dateien in einem geschützten Ordner wieder in ihren normalen, entschlüsselten Zustand zurückversetzt.

Alle Dateien und Ordner des geschützten Ordners werden entschlüsselt und die Kennzeichnung der Dateien mit dem PGP-Symbol wird entfernt.

So entfernen Sie den Schutz eines durch PGP NetShare geschützten Ordners

1 Wählen Sie im Bildschirm „PGP NetShare“ den geschützten Ordner aus, dessen Schutz Sie entfernen möchten.

2 Klicken Sie links im Hauptbildschirm von PGP Desktop im Bedienfeld „PGP NetShare“ auf **Ordner entfernen**. Das Dialogfeld „Entschlüsselung bestätigen“ wird angezeigt.

3 Vergewissern Sie sich, dass Sie den richtigen Ordner ausgewählt haben, und klicken Sie auf **Weiter**. Falls die Passphrase nicht zwischengespeichert wurde, wird das Dialogfeld zum Entsperren des Ordners angezeigt.

4 Geben Sie die Passphrase eines der Schlüssel ein, an den die Dateien verschlüsselt wurden, und klicken Sie auf **OK**. Geben Sie eine entsprechende Passphrase innerhalb der zulässigen Zeit ein, da die Entschlüsselung andernfalls abgebrochen wird. Die Fortschrittsanzeige wird angezeigt und die Dateien werden entschlüsselt.

5 Klicken Sie auf **Beenden**. Die Dateien im geschützten Ordner sind nun nicht mehr durch Verschlüsselung geschützt. Der Ordner wird aus der Liste der durch PGP NetShare geschützten Ordner entfernt und das Sperrsymbol wird ausgeblendet.

Tipp: Sie können einen Ordner auch entschlüsseln, indem Sie in Windows Explorer mit der rechten Maustaste darauf klicken und im Kontextmenü die Option **Ordner aus PGP NetShare entfernen** auswählen.

Ordner umschlüsseln

Bei der Umschlüsselung eines Ordners werden die Dateien im angegebenen geschützten Ordner umgeschlüsselt. Dabei wird der zugrunde liegende Schlüssel geändert, sodass keine Personen Zugriff erhalten, die den aktuellen Schlüssel möglicherweise in Erfahrung gebracht haben. Sie müssen ein Gruppenadministrator oder Administrator des Ordners sein, um ihn umschlüsseln zu können.

Der Befehl „Ordner umschlüsseln“ kann zu einem beliebigen Zeitpunkt aufgerufen werden, z. B. wenn Sie vermuten, dass eine unbefugte Person Zugriff auf die Dateien im geschützten Ordner erlangt hat.

Gründe für ein Umschlüsseln sind z. B.:

- Sie befürchten, dass ein Teil des Inhalts eines geschützten Ordners nicht verschlüsselt ist, wenn z. B. ein unbefugter Benutzer eine Datei in einem geschützten Ordner ablegt.
- Die Sicherheit der Schlüsselinformationen eines autorisierten Benutzers ist nicht mehr gewährleistet.
- Ein neuer autorisierter Benutzer wurde hinzugefügt und benötigt Zugriff auf den geschützten Ordner (dies geschieht nicht automatisch).

So schlüsseln Sie einen geschützten Ordner um

1. Wählen Sie im Bildschirm „PGP NetShare“ den geschützten Ordner aus, dessen Schutz Sie entfernen möchten.
2. Klicken Sie auf der linken Seite des Fensters von PGP Desktop im Bedienfeld „PGP NetShare“ auf **Ordner umschlüsseln**. Der Bildschirm „Benutzer hinzufügen“ wird angezeigt.

   Wird ein geschützter Ordner umgeschlüsselt, können Sie diesem neue Mitglieder hinzufügen oder vorhandene Mitglieder entfernen.
3. Klicken Sie auf **Weiter**, um fortzufahren. Der Bildschirm „Signierer auswählen“ wird angezeigt.
4. Wählen Sie aus den privaten Schlüsseln am lokalen Schlüsselbund einen Schlüssel aus oder akzeptieren Sie den Standardschlüssel. Dieser Schlüssel dient bei der Umschlüsselung zum Signieren der Dateien.
5. Geben Sie nach der entsprechenden Aufforderung die Passphrase ein und klicken Sie auf **Weiter**. Die Fortschrittsanzeige wird angezeigt und die Dateien im angegebenen geschützten Ordner werden umgeschlüsselt.
6. Klicken Sie auf **Beenden**. Der Umschlüsselungsvorgang ist abgeschlossen.

Passphrasen löschen

Standardmäßig werden Passphrasen von PGP NetShare entsprechend der Einstellungen auf der Registerkarte „Allgemein“ der PGP Desktop-Optionen zwischengespeichert. Dies erleichtert die Verwendung von PGP NetShare, da Sie beim Zugriff auf die Dateien im geschützten Ordner die Passphrase nicht eingeben müssen.

Wenn Sie jedoch Ihrem Platz am System verlassen, ist eine zwischengespeicherte Passphrase nicht empfehlenswert, da eine unbefugte Person Aktionen durchführen könnte, ohne die Passphrase zu benötigen.

So löschen Sie eine Passphrase

1. Klicken Sie in Windows auf das PGP-Symbol in der Taskleiste.
2. Wählen Sie im angezeigten Menü die Option **Caches löschen** aus. Damit dieser Befehl verfügbar ist, muss mindestens eine Passphrase zwischengespeichert sein. Die zwischengespeicherten Passphrasen werden gelöscht.

Dateien außerhalb eines geschützten Ordners schützen

PGP NetShare verfügt über eine erweiterte Option, mit der Sie einzelne Dateien schützen können, die sich *nicht* in einem durch PGP NetShare geschützten Ordner befinden. Diese Option ist standardmäßig deaktiviert.

Hinweis: Der PGP-Administrator hat diese Option u. U. deaktiviert, wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung verwenden.

Damit Sie einzelne Dateien außerhalb eines durch PGP NetShare geschützten Ordners schützen können, müssen Sie zunächst in den PGP-Optionen auf der Registerkarte „NetShare“ die Option **Einzelne Dateien schützen auswählen. Weitere Informationen finden Sie unter** *PGP NetShare-Optionen* (auf Seite 340). Wenn diese Option nicht aktiviert ist, können Sie Dateien, die sich außerhalb eines durch PGP NetShare geschützten Ordners befinden, nicht schützen.

Wenn Sie die Option **Einzelne Dateien schützen** aktiviert haben, können Sie einzelne Dateien außerhalb eines geschützten Ordners schützen, indem Sie in Windows Explorer das Kontextmenü von PGP Desktop verwenden. *Einzeln geschützte Dateien werden nicht im PGP NetShare-Arbeitsbereich der Benutzeroberfläche von PGP Desktop angezeigt.*

Achtung: PGP NetShare versucht, einzeln geschützte Dateien effektiv zu schützen. Einige Anwendungen (z. B. Microsoft Word) speichern geänderte Dateien jedoch so, dass PGP NetShare annimmt, die geschützte Datei wäre gelöscht worden. Unter diesen Umständen ist PGP NetShare nicht in der Lage, diese Dateien weiterhin zu schützen. Beachten Sie, dass dies nur für einzeln geschützte Dateien gilt, die sich nicht in einem geschützten Ordner befinden, und nicht für Dateien in einem geschützten PGP NetShare-Ordner. Damit der Schutz geschützter Dateien nicht aufgehoben wird, empfiehlt die PGP Corporation eindringlich, zu schützende Dateien in einem durch PGP NetShare geschützten Ordner zu behalten.

So aktivieren Sie die Option „Einzelne Dateien schützen“

1. Klicken Sie auf **Extras > PGP-Optionen**.
2. Klicken Sie auf die Registerkarte **NetShare**.
3. Vergewissern Sie sich auf der Registerkarte „NetShare“, dass die Option **Einzelne Dateien schützen** aktiviert ist. Standardmäßig ist diese Einstellung *nicht* aktiviert.

So schützen Sie einzelne Dateien mit PGP NetShare

1. Klicken Sie in Windows Explorer mit der rechten Maustaste auf die Datei, die Sie mit PGP NetShare schützen möchten.
2. Wählen Sie im Kontextmenü die Option **PGP Desktop > [Dateiname] zu PGP NetShare hinzufügen** aus.
3. Fügen Sie im PGP NetShare-Assistenten autorisierte Benutzer hinzu und wählen Sie einen privaten Schlüssel zum Signieren aus.
4. Klicken Sie nach Abschluss des Verschlüsselungsvorgangs auf **Fertig stellen**. Die geschützte Datei wird in Windows Explorer mit einem PGP NetShare-Symbol angezeigt.

Sie können über das Kontextmenü auch die PGP NetShare-Eigenschaften einer geschützten Datei anzeigen, einzeln geschützte Dateien umschlüsseln, die sich außerhalb eines geschützten Ordners befinden, und den Schutz dieser Dateien aufheben.

So zeigen Sie die PGP NetShare-Eigenschaften einer geschützten Datei über das Kontextmenü an

1. Klicken Sie in Windows Explorer mit der rechten Maustaste auf die geschützte Datei, deren PGP NetShare-Eigenschaften Sie anzeigen möchten.
2. Wählen Sie im Kontextmenü die Option **PGP Desktop > PGP NetShare-Eigenschaften.** Das Eigenschaftenfenster der ausgewählten Datei wird angezeigt.
3. Klicken Sie zum Schließen des Eigenschaftenfensters auf **OK**.

So schlüsseln Sie geschützte Dateien über das Kontextmenü um

1. Klicken Sie in Windows Explorer mit der rechten Maustaste auf die geschützte Datei, die Sie umschlüsseln möchten.
2. Wählen Sie im Kontextmenü die Option **PGP Desktop > Umschlüsseln aus.**
3. Fügen Sie im PGP NetShare-Assistenten autorisierte Benutzer hinzu und/oder entfernen Sie diese und wählen Sie einen privaten Schlüssel zum Signieren aus.
4. Wenn der Umschlüsselungsvorgang abgeschlossen ist, klicken Sie auf **Fertig stellen**.

So heben Sie den Schutz einzeln geschützter Dateien über das Kontextmenü auf

1. Klicken Sie in Windows Explorer mit der rechten Maustaste auf die geschützte Datei, deren Schutz Sie aufheben möchten.
2. Wählen Sie im Kontextmenü die Option **PGP Desktop > [Dateiname] aus PGP NetShare entfernen** aus.
3. Bestätigen Sie im PGP NetShare-Assistenten, dass Sie den Schutz dieser Datei aufheben möchten, indem Sie auf **Weiter** klicken.
4. Wenn die Datei entschlüsselt wurde, klicken Sie auf **Fertig stellen**.

Sicherungskopien für durch PGP NetShare geschützte Dateien erstellen

Sie können Dateien und Ordner sichern, die durch PGP NetShare geschützt wurden. Die Handhabung der Dateien während der Sicherung wird dadurch bestimmt, ob Sie PGP NetShare in einer von einem PGP Universal Server verwalteten Umgebung verwenden oder nicht.

Sicherungskopien von Dateien mit einem nicht verwalteten Client erstellen

Wenn ein nicht in einer verwalteten Umgebung arbeitender (eigenständiger) Client geschützte Dateien und Ordner sichert, werden die geschützten Dateien beim Sichern transparent entschlüsselt und als Klartext auf dem Sicherungsmedium gespeichert. Beim Wiederherstellen der ursprünglichen Verschlüsselung werden sie transparent verschlüsselt.

Sicherungskopien von Dateien mit einem von einem PGP Universal Server verwalteten Client erstellen

Wenn ein verwalteter Client zum Sichern geschützter Dateien und Ordner verwendet wird, ist die Handhabung der Verschlüsselung davon abhängig, ob die Sicherungsanwendung vom PGP Universal Server-Administrator als Anwendungsumgehung eingerichtet wurde.

- Gehört die Sicherungsanwendung zur Umgehungsliste für die Entschlüsselung, bleiben die geschützten Dateien nach der Sicherung auf dem Sicherungsmedium verschlüsselt. Beim Wiederherstellen am ursprünglichen Speicherort bleiben sie weiterhin verschlüsselt.
- Gehört die Sicherungsanwendung nicht zur Umgehungsliste für die Entschlüsselung, gleicht der Vorgang dem Sichern von Dateien mit einem Client in einer nicht verwalteten Umgebung. In diesem Fall werden die geschützten Dateien während der Sicherung transparent entschlüsselt und auf dem Sicherungsmedium als Klartext gespeichert. Beim Wiederherstellen der ursprünglichen Verschlüsselung werden sie transparent verschlüsselt.

Hinweis: Die PGP Corporation empfiehlt, dass Sie die verschiedenen Szenarien beim Sichern und Wiederherstellen von Daten nicht kombinieren. Wenn Sie beispielsweise einen Client in einer nicht verwalteten Umgebung zum Sichern der Dateien verwenden, sollten Sie die Dateien auch mit einem Client in einer nicht verwalteten Umgebung wiederherstellen.

Mithilfe des Kontextmenüs auf PGP NetShare-Funktionen zugreifen

Bestimmte PGP NetShare-Funktionen sind in den Kontextmenüs von Windows Explorer verfügbar.

Sie können Ordner (und Dateien, wenn Sie die Option **Einzelne Dateien schützen** aktiviert haben) über Windows Explorer schützen, indem Sie mit der rechten Maustaste auf den Ordner bzw. die Datei klicken. Wählen Sie im Kontextmenü die Option **PGP Desktop > [Name] zu PGP NetShare hinzufügen** aus, um den Ordner bzw. die Datei für den Schutz durch PGP NetShare zu kennzeichnen.

Weitere Informationen zum Schützen einzelner Dateien außerhalb eines geschützten Ordners mit PGP NetShare finden Sie unter *Dateien außerhalb eines geschützten Ordners schützen* (auf Seite 277).

Wenn ein Ordner oder eine Datei durch PGP NetShare geschützt ist, stehen im Kontextmenü von Windows Explorer drei Befehle zur Verfügung:

- **PGP NetShare-Eigenschaften**: Mit diesem Befehl wird für die Datei bzw. den Ordner das Dialogfeld „Eigenschaften“ mit der Registerkarte „PGP NetShare“ geöffnet. Auf dieser Registerkarte können Sie anzeigen, welche Benutzer geschützte Dateien nutzen, gesperrte Dateien und Ordner freigeben und Benutzer zum Verwenden der geschützten Dateien hinzufügen dürfen.
- **Umschlüsseln**: Mit diesem Befehl wird der angegebene Ordner oder die Datei an einen neuen zugrunde liegenden Schlüssel umgeschlüsselt.
- **<Dateiname> aus PGP NetShare entfernen**: Mit diesem Befehl wird der PGP NetShare-Schutz des angegebenen Ordners oder der Datei entfernt.

Die entsprechenden Verfahren finden Sie unter *Dateien außerhalb eines geschützten Ordners schützen* (auf Seite 277).

PGP NetShare in einer von einem PGP Universal Server verwalteten Umgebung

Wenn Sie PGP NetShare in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, hat der PGP-Administrator möglicherweise Einstellungen konfiguriert, die sich auf das Verhalten von PGP NetShare auf Ihrem System auswirken.

Dies kann folgende Einstellungen umfassen:

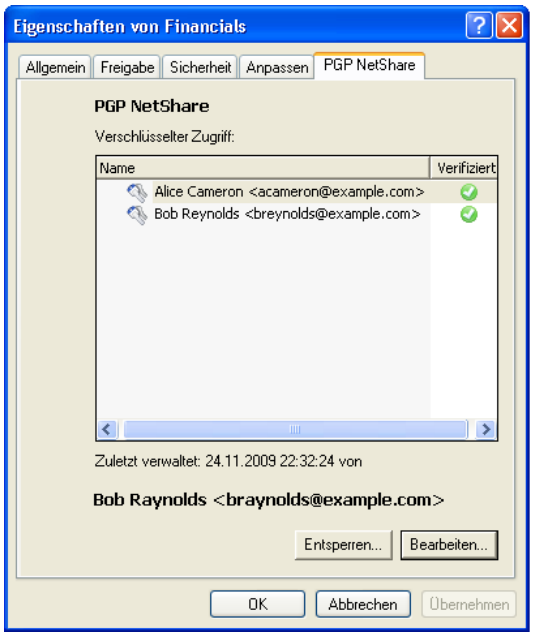
- **Der Benutzer darf PGP NetShare-Ordner erstellen und verwalten**: Wenn diese Einstellung aktiviert ist, können Sie Ordner erstellen, die durch PGP NetShare geschützt sind. Ist die Einstellung deaktiviert, können Sie geschützte Ordner verwenden, die andere Personen erstellt haben, jedoch können Sie selbst keine geschützten Ordner erstellen. Diese Einstellung ist standardmäßig aktiviert.
- **Der Benutzer darf den erweiterten Benutzermodus aktivieren**: Wenn diese Einstellung aktiviert ist, können Sie in den PGP-Optionen den erweiterten Benutzermodus aktivieren. Das bedeutet, dass Sie einzelne Dateien schützen können, die sich nicht mehr in einem geschützten Ordner befinden. Diese Einstellung ist standardmäßig deaktiviert.
- **Die Verschlüsselung von Dateien in den folgenden Ordnern erzwingen**: Diese Ordner werden als auf der Positivliste aufgeführte Ordner bezeichnet. Positiv gelistete Ordner sind Ordner, die *immer* zu PGP NetShare hinzugefügt und verschlüsselt werden. Weitere Informationen finden Sie unter *Vom PGP Universal Server festgelegte negativ oder positiv gelistete Ordner* (auf Seite 256).

- **Die Verschlüsselung von Dateien in den folgenden Ordnern verhindern**: Diese Ordner werden als negativ gelistete Ordner bezeichnet. Negativ gelistete Ordner sind Ordner, die *nie* zu PGP NetShare hinzugefügt und verschlüsselt werden. Weitere Informationen finden Sie unter *Vom PGP Universal Server festgelegte negativ oder positiv gelistete Ordner* (auf Seite 256).

Wenden Sie sich an den PGP-Administrator, wenn Sie Fragen zu diesen Einstellungen haben.

Auf die Eigenschaften geschützter Dateien oder Ordner zugreifen

Für jede durch PGP NetShare geschützte Datei wird im Bildschirm „Eigenschaften“ eine Registerkarte „PGP NetShare“ mit Informationen zur Datei angezeigt.



So greifen Sie auf die Registerkarte „PGP NetShare“ im Dialogfeld „Eigenschaften“ einer Datei zu

1 Führen Sie in Windows Explorer einen der folgenden Schritte aus:

- Klicken Sie mit der rechten Maustaste auf die Datei und wählen Sie im Kontextmenü die Option **Eigenschaften** aus.
- Klicken Sie auf **Datei > Eigenschaften**.

Der Bildschirm mit den Eigenschaften der ausgewählten Datei wird angezeigt.

2 Klicken Sie auf die Registerkarte **PGP NetShare**. Die Registerkarte „PGP NetShare“ wird angezeigt.

3 Auf dieser Registerkarte werden die Namen der Benutzer aufgeführt, die die verschlüsselte Datei verwenden können. Sie haben folgende Möglichkeiten:

- **Entsperren**: Klicken Sie hier, um einen geschützten Ordner zu entsperren, der gesperrt wurde.
- **Bearbeiten**: Klicken Sie hier, um den Bildschirm „Benutzer hinzufügen“ anzuzeigen, über den Sie Benutzer hinzufügen oder entfernen können, die auf den ausgewählten Ordner bzw. die Datei zugreifen dürfen. Die Datei bzw. der Ordner wird umgeschlüsselt, wenn ein Benutzer hinzugefügt oder entfernt wird.
- Zeigen Sie die Rollen der einzelnen Benutzer an, indem Sie mit der rechten Maustaste auf den Benutzernamen klicken. Es ist auf dieser Registerkarte nicht möglich, die Rolle des Benutzers zu ändern (weitere Informationen zum Ändern von Benutzerrollen finden Sie unter *Benutzerrollen ändern* (siehe "Rollen von Benutzern ändern" auf Seite 270)).

4 Klicken Sie auf **OK**, um das Dialogfeld „Eigenschaften“ zu schließen.

PGP NetShare-Menüs in PGP Desktop verwenden

Es gibt in PGP Desktop drei Menüs mit Befehlen, die PGP NetShare betreffen: „Datei“, „Bearbeiten“ und „NetShare“.

Menü „Datei“

Wenn das Bedienfeld „PGP NetShare“ ausgewählt ist, können Sie mit dem Befehl **Datei > Neuer PGP NetShare-Ordner** einen neuen geschützten Ordner erstellen.

Das Verfahren ist identisch mit der Beschreibung unter *Neue durch PGP NetShare geschützte Ordner erstellen* (auf Seite 260).

Menü „Bearbeiten“

Wenn das Bedienfeld „PGP NetShare“ ausgewählt ist, können Sie mit dem Befehl **Umbenennen** im Menü „Bearbeiten“ von PGP Desktop einen geschützten Ordner umbenennen.

So benennen Sie einen durch PGP NetShare geschützten Ordner über das Menü „Bearbeiten“ um

1. Öffnen Sie PGP Desktop und klicken Sie auf das Bedienfeld **PGP NetShare**.
2. Wenn mehrere geschützte Ordner vorhanden sind, klicken Sie auf den Namen des geschützten Ordners, den Sie umbenennen möchten.
3. Klicken Sie auf **Bearbeiten > Umbenennen**.
4. Geben Sie einen neuen Namen für den geschützten Ordner ein.
5. Drücken Sie die **Eingabetaste** oder klicken Sie außerhalb des Namens des geschützten Ordners. Der geschützte Ordner wird umbenannt.

Der Befehl **Datei in Explorer anzeigen** im Menü „Bearbeiten“ entspricht dem Klicken auf den Pfad eines geschützten Ordners. Der ausgewählte Ordner wird dann in Windows Explorer geöffnet.

Menü „NetShare“

Wenn das Bedienfeld „PGP NetShare“ ausgewählt ist, stehen im Menü „NetShare“ folgende Befehle zur Verfügung:

- **Ordner hinzufügen**: Wählen Sie diesen Befehl aus, um einen neuen geschützten Ordner zu erstellen. Das Verfahren ist identisch mit der Beschreibung unter *Neue durch PGP NetShare geschützte Ordner erstellen* (auf Seite 260). Das Bedienfeld „PGP NetShare“ muss ausgewählt sein, damit dieser Befehl aktiv ist.
- **Ordner entfernen**: Wählen Sie diesen Befehl aus, wenn Sie einen geschützten Ordner wieder in seinen normalen, unverschlüsselten Zustand zurückversetzen möchten. Alle Dateien und Ordner im geschützten Ordner werden entschlüsselt und die Kennzeichnung der Dateien mit dem PGP-Symbol wird entfernt. Sie müssen einen geschützten Ordner auswählen, damit dieser Befehl aktiv ist.
- **Ordner umschlüsseln**: Wählen Sie diesen Befehl aus, um die Dateien in einem geschützten Ordner umzuschlüsseln. Dabei wird der zugrunde liegende Schlüssel geändert, sodass keine Personen Zugriff erhalten, die den aktuellen Schlüssel möglicherweise in Erfahrung gebracht haben. Die Umschlüsselung erfolgt automatisch, wenn ein Benutzer einem geschützten Ordner hinzugefügt oder daraus entfernt wird. Der Befehl **Ordner umschlüsseln** kann zu einem beliebigen Zeitpunkt aufgerufen werden, z. B. wenn Sie vermuten, dass eine unbefugte Person Zugriff auf die Dateien im geschützten Ordner erlangt hat. Sie müssen einen geschützten Ordner auswählen, damit dieser Befehl aktiv ist.
- **Ordnerstatus prüfen**: Wählen Sie diesen Befehl aus, um die aktuellsten Informationen zum Status des ausgewählten geschützten Ordners abzurufen. Sie müssen einen geschützten Ordner auswählen, damit dieser Befehl aktiv ist.

- **Letzten Ordner löschen**: Wählen Sie diesen Befehl aus, um den ausgewählten Ordner aus der Liste der geschützten Ordner zu entfernen. Im Gegensatz zum Befehl **Ordner entfernen** werden die Dateien im geschützten Ordner nicht entschlüsselt. Sie müssen einen geschützten Ordner auswählen, damit dieser Befehl aktiv ist.

14 PGP Zip verwenden

Mit PGP Zip können Sie verschlüsselte und komprimierte Pakete, so genannte PGP Zip-Archive, erstellen, öffnen und bearbeiten. In diesem Abschnitt werden die PGP Zip-Funktionen von PGP Desktop erläutert.

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung verwenden, hat Ihr PGP Universal Server-Administrator ggf. bestimmte Funktionen deaktiviert. Ist eine Funktion deaktiviert, wird das Bedienelement auf der linken Seite nicht angezeigt und das Menü oder andere auf diese Funktion zutreffenden Optionen sind nicht verfügbar. Die in diesem Handbuch enthaltenen Abbildungen entsprechen der Standardinstallation, bei der alle Funktionen aktiviert sind. Wenn Ihr PGP Universal Server-Administrator diese Funktion deaktiviert hat, ist dieser Abschnitt für Sie nicht relevant.

In diesem Kapitel

Übersicht 287
PGP Zip-Archive erstellen 288
PGP Zip-Archive öffnen 299
PGP Zip-SDAs öffnen 300
PGP Zip-Archive bearbeiten 301
Signierte PGP Zip-Archive verifizieren 303

Übersicht

Ein PGP Zip-Archiv (Paket) ist eine einzelne Datei, die zur einfachen Datenübertragung und -sicherung komprimiert ist. Diese Archivdateien können eine beliebige Kombination von Dateien und/oder Ordnern enthalten und sind besonders für die Datenübertragung oder Datensicherung geeignet.

Verwenden Sie den PGP Zip-Assistenten, um neue PGP Zip-Archive zu erstellen. Der Assistent leitet Sie durch das Verfahren zur Auswahl von Dateien und/oder Ordnern für das Archiv sowie zur Verschlüsselung und Komprimierung:

- Verschlüsselung und Komprimierung von Dateien und/oder Ordnern mithilfe der PGP-Schlüssel eines oder mehrerer Empfänger (auf den Computern der Empfänger muss PGP Desktop installiert sein).

- Verschlüsselung und Komprimierung von Dateien und/oder Ordnern mithilfe einer Passphrase (auf den Computern der Empfänger muss PGP Desktop installiert sein).
- Verschlüsselung und Komprimierung von Dateien und/oder Ordner in ein selbstentschlüsselndes Archiv (PGP Zip-SDA), das durch eine Passphrase geschützt ist (die Empfänger benötigen PGP Desktop nicht, auf den Computern muss jedoch Microsoft Windows installiert sein).
- Keine Verschlüsselung und Komprimierung, stattdessen wird eine Datei erstellt, die Sie an die Empfänger senden und die Sie als Absender der Datei identifiziert.

Wenn Sie den PGP Zip-Assistenten zum Erstellen eines PGP Zip-Archivs verwenden, können Sie die Originaldateien automatisch an PGP Shredder senden lassen, sodass diese Dateien sicher und dauerhaft vom Computer gelöscht werden.

Wenn Sie eine PGP Zip-Archivdatei erhalten, können Sie Folgendes tun:

- Alle Dateien und/oder Ordner aus dem Archiv extrahieren.
- Bestimmte Dateien und/oder Ordner aus dem Archiv extrahieren.
- Bestimmte Dateien und/oder Ordner aus dem Archiv extrahieren und andere Dateien und/oder Ordner hinzufügen.
- Dem Archiv neue Dateien und/oder Ordner hinzufügen.
- Bearbeiten Sie das Archiv, indem Sie folgendermaßen vorgehen:
  - Das Verschlüsselungsverfahren ändern.
  - Den Signaturschlüssel ändern.
  - Die Empfänger ändern.

PGP Zip-Archive werden an den bevorzugten Algorithmus Ihrer Kopie von PGP Desktop (sofern diese von einem PGP Universal Server-Administrator konfiguriert wurde) oder an AES-256 verschlüsselt. PGP Zip-Archive können zwischen Windows- und Mac OS X-Plattformen verschoben werden. PGP Desktop muss auf dem Computer installiert sein, auf den ein PGP Zip-Archiv übertragen werden soll.

PGP Zip-Archive erstellen

So erstellen Sie ein PGP Zip-Archiv

1. Klicken Sie auf das Bedienfeld „PGP Zip“ und dann auf **Neues PGP Zip-Archiv**. Der PGP Zip-Assistent wird angezeigt.
2. Führen Sie einen der folgenden Schritte aus:
   - Ziehen Sie die Dateien in den im Assistenten gekennzeichneten Bereich.

- Wenn Sie ein gesamtes Verzeichnis in ein PGP Zip-Archiv einfügen möchten, klicken Sie auf **Verzeichnis hinzufügen** .
- Wenn Sie eine Datei in ein PGP Zip-Archiv einfügen möchten, klicken Sie auf **Dateien hinzufügen** .
- Wenn Sie eine Datei oder ein Verzeichnis aus dem PGP Zip-Archiv entfernen möchten, klicken Sie auf **Ausgewählte Dateien entfernen** .
- Wenn Sie zusätzliche Optionen für die PGP Zip-Datei auswählen möchten, klicken Sie auf **Erweiterte PGP Zip-Optionen** . Die Standardeinstellungen eignen sich für die meisten Benutzer.

Hinweis: Wenn Sie sowohl Dateien als auch Ordner hinzufügen möchten, verwenden Sie eine Kombination der Schaltflächen und . Wenn Sie der Dateiliste ein Verzeichnis hinzufügen, zeigt der PGP Zip-Assistent die Dateien einzeln an, um die Übersicht zu erleichtern. Wenn Sie dem PGP Zip-Archiv viele Dateien hinzufügen möchten, können Sie Zeit sparen, indem Sie der Dateiliste des PGP Zip-Archivs zunächst ein gesamtes Verzeichnis hinzufügen und dann die Dateien entfernen, die nicht hinzugefügt werden sollen. *Bei diesem Vorgehen sollten Sie sich vor dem nächsten Schritt vergewissern, dass Sie tatsächlich alle Dateien entfernt haben, die nicht für das PGP Zip-Archiv vorgesehen sind.*

3 Wenn Sie die Originaldateien nach dem Erstellen des PGP Zip-Archivs sicher löschen möchten, wählen Sie die Option **Nach Abschluss Originaldateien an PGP Shredder senden aus.**

Achtung: Dateien, die nach der Erstellung des PGP Zip-Archivs an PGP Shredder gesendet werden, können selbst mit einem entsprechenden Dienstprogramm nicht mehr abgerufen werden. Die Dateien werden dauerhaft gelöscht und können nicht wiederhergestellt werden. Setzen Sie diese Option also mit Vorsicht ein.

4 Legen Sie spezielle Optionen fest, indem Sie auf **Erweiterte PGP Zip-Optionen** klicken:

- Wenn Sie einzelne verschlüsselte Dateien erstellen möchten und nicht ein umfassendes PGP Zip-Archiv, das alle Dateien in einer einzelnen verschlüsselten Datei umfasst, wählen Sie **Kein Zip-Archiv erstellen (Dateien einzeln ausgeben)** aus.
- Wenn Sie Zip-Archive ausschließlich aus Textdateien erstellen möchten, aktivieren Sie die Option **Zeilenwechselzeichen für Textdateien konvertieren** aus.

- Wenn Sie ein Zip-Archiv erstellen möchten, für das PGP Secure Viewer erforderlich ist (entsprechend einer eventuell durch die Sicherheitsrichtlinien Ihres Unternehmens definierten Anforderung), wählen Sie **PGP Secure Viewer auch beim Entschlüsseln erfordern** aus. In diesem Modus wird die Datei beim Entschlüsseln in einem PGP Secure Viewer-Fenster angezeigt. Diese Option schützt gegen veraltete Angriffe, bei denen Strahlung abgefangen wird.
- Wenn Sie das Zip-Archiv als binäre Datei in einer E-Mail-Nachricht versenden möchten und eine ältere E-Mail-Anwendung verwenden, wählen Sie die Option **Textausgabe** aus. Durch das Speichern der Datei als ASCII-Text wird die verschlüsselte Datei um ca. 30 Prozent größer. Diese Option ist nicht verfügbar, wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen.
- Wenn Sie diese PGP Zip-Optionen für die zukünftige Verwendung speichern möchten, wählen Sie die Option **Einstellungen beim nächsten Mal wieder verwenden** aus.
- Klicken Sie auf **OK**, wenn Sie alle speziellen Optionen ausgewählt haben. Klicken Sie auf **Abbrechen**, wenn Sie keine der Optionen ändern möchten.

Das Dialogfeld „Neues PGP Zip-Archiv“ wird wieder angezeigt.

5 Nachdem Sie alle Dateien für das PGP Zip-Archiv ausgewählt haben, klicken Sie auf **Weiter**.

6 Wählen Sie die gewünschte Verschlüsselungsmethode aus und klicken Sie auf **Weiter**.

Tipp: Zeigen Sie mit der Maus auf die einzelnen Optionen, um im Informationsfeld unter der Liste weitere Details anzuzeigen.

- **Empfängerschlüssel**: Erstellt ein PGP Zip-Archiv, indem die Dateien an die öffentlichen Schlüssel der Empfänger verschlüsselt werden. Dadurch wird gewährleistet, dass nur diese Empfänger mithilfe von PGP Desktop das Archiv öffnen können. Diese Option bietet den zuverlässigsten Schutz. Weitere Informationen finden Sie unter *Verschlüsselung an Empfängerschlüssel* (auf Seite 291).
- **Passphrase**: Erstellt ein PGP-Zip-Archiv, indem die Dateien mit einer Passphrase verschlüsselt werden, die Sie beim Speichern des Archivs festlegen. Das Archiv kann nur von Personen geöffnet werden, die die Passphrase kennen und PGP Desktop zum Öffnen des Archivs verwenden. Weitere Informationen finden Sie unter *Verschlüsselung mit Passphrasen* (auf Seite 293).

- **Selbstentschlüsselndes PGP-Archiv: Erstellt ein selbstentschlüsselndes PGP-Archiv mit einer Passphrase, die Sie beim Speichern des Archivs festlegen. PGP Desktop ist zum Entschlüsseln eines selbstentschlüsselnden PGP-Archivs nicht erforderlich. Die Empfänger** *müssen* jedoch einen Computer mit Microsoft Windows verwenden. Weitere Informationen finden Sie unter *Selbstentschlüsselnde PGP-Archive (SDA) erstellen* (auf Seite 296).
- **Nur signieren**: Fügt einer unverschlüsselten Zip-Datei Ihre PGP-Signatur hinzu. Die Empfänger können das Zip-Archiv mit PGP Desktop öffnen. Durch die Signatur wird gewährleistet, dass das Archiv von Ihnen stammt und während der Übertragung nicht verändert wurde. Weitere Informationen finden Sie unter *Nur signieren* (siehe "Ein Archiv nur mit Signatur erstellen" auf Seite 298).

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, ist die (konventionelle) Verschlüsselung mit Passphrasen möglicherweise deaktiviert.

Verschlüsselung an Empfängerschlüssel

Verwenden Sie **Empfängerschlüssel** in folgenden Fällen:

- Um den höchsten Grad an Sicherheit für Ihre Dateien zu erreichen.
- Wenn alle Empfänger PGP Desktop auf ihren Computern (Windows oder Mac OS X) installiert haben.
- Wenn Sie für jeden Empfänger über einen öffentlichen Schlüssel verfügen (gespeichert an Ihrem Schlüsselbund oder auf einem PGP-Keyserver).
- Wenn Sie den Empfängern keine Passphrase mitteilen möchten.

Die Verschlüsselung eines PGP Zip-Archivs mit den öffentlichen Schlüssel aller Empfänger ist die sicherste Variante und sollte grundsätzlich immer verwendet werden, wenn höchste Sicherheit gewährleistet sein muss und die erforderlichen Voraussetzungen erfüllt sind.

Sobald die Dateien geschützt sind, senden Sie die entstandene PGP Zip-Archivdatei an die gewünschten Empfänger. Die Empfänger öffnen die PGP Zip-Archivdatei dann mit PGP Desktop. Alle, deren Schlüssel Sie bei der Verschlüsselung der Datei eingebunden haben, können die PGP Zip-Archivdatei öffnen. Alle Benutzer können auf dieselben Objekte zugreifen. Wenn Sie möchten, dass einige Empfänger nur auf bestimmte Objekte zugreifen können, müssen Sie für jeden Empfänger ein eigenes PGP Zip-Archiv erstellen.

So verschlüsseln Sie an Empfängerschlüssel

1 Sofern Sie diesen Schritt noch nicht ausgeführt haben, erstellen Sie ein PGP Zip-Archiv gemäß der Anleitung unter *PGP Zip-Archive erstellen* (auf Seite 288).

2 Wählen Sie im Dialogfeld „Verschlüsseln“ die Option **Empfängerschlüssel** aus.

3 Klicken Sie auf **Weiter**. Das Dialogfeld „Benutzerschlüssel hinzufügen“ wird angezeigt.

4 Wählen Sie die Empfänger des PGP Zip-Archivs aus. Führen Sie einen der folgenden Schritte aus:

- Wenn Sie eine Auswahl aus der Liste der Schlüssel am Schlüsselbund treffen möchten, klicken Sie auf den Pfeil.
- Wenn Sie die Datei an einen Empfänger senden möchten, dessen Schlüssel sich nicht am Schlüsselbund befindet, klicken Sie auf **Hinzufügen**. Das Dialogfeld „Empfängerauswahl“ wird angezeigt.

Wenn Sie alle zusätzlichen Namen ausgewählt haben, klicken Sie auf **OK**, um zum Fenster **Benutzerschlüssel hinzufügen** zurückzukehren.

Wenn Sie einen Schlüssel entfernen möchten, wählen Sie den Namen des Empfängers aus und klicken Sie auf **Entfernen**.

5 Klicken Sie auf **Weiter**. **Der Bildschirm „Signieren und Speichern“ wird angezeigt.**

6 Auf Wunsch können Sie einen privaten Schlüssel am Schlüsselbund als Signaturschlüssel für das zu erstellende PGP Zip-Archiv angeben.

Dieser Signaturschlüssel wird verwendet, um das PGP Zip-Archiv digital zu signieren. Die Empfänger können die Herkunft des Archivs verifizieren, indem sie die digitale Signatur mit dem zugehörigen öffentlichen Schlüssel verifizieren.

- Wenn die Datei nicht signiert werden muss oder soll, wählen Sie in der Liste „Signaturschlüssel“ den Eintrag **Keiner** aus.
- Wenn Sie das PGP Zip-Archiv signieren möchten, wählen Sie Ihren Schlüssel aus der Signaturschlüsselliste aus und geben Sie die Passphrase des ausgewählten Signaturschlüssels ein (dies ist nicht die Passphrase, die zur Sicherung der Zip-Datei verwendet wird). Wenn die eingegebenen Zeichen bei der Passphraseneingabe angezeigt werden sollen, wählen Sie **Tastatureingabe anzeigen** aus.

Wenn Sie die Passphrase im Verlauf dieser Sitzung bereits mit PGP Desktop eingegeben haben, ist die Passphrase eventuell zwischengespeichert. Maßgebend sind hierbei die Einstellungen unter **Optionen**. In diesem Fall wird eine Meldung angezeigt, dass die Passphrase zwischengespeichert ist. Selbst wenn die Passphrase zwischengespeichert ist, können Sie entscheiden, die PGP Zip-Archivdatei nicht zu signieren.

7 Bestätigen Sie, dass das PGP Zip-Archiv am angegebenen Speicherort unter dem eingegebenen Dateinamen gespeichert wird. Bei Bedarf haben Sie folgende Möglichkeiten:

- Ändern Sie den Speicherort der Datei, indem Sie auf **Durchsuchen** klicken und im Windows-Dialogfeld „Datei“ einen anderen Speicherort auswählen.
- Ändern Sie den Speicherort der Datei, indem Sie manuell den Speicherort für das PGP Zip-Archiv eingeben.
- Ändern Sie den Namen der PGP Zip-Archivdatei, indem Sie ihn am Ende der Zeichenfolge des Dateispeicherorts eingeben.

Der Standarddateiname für ein PGP Zip-Archiv, das nur eine einzige Datei, ein einziges Verzeichnis oder ein einziges Laufwerk enthält, setzt sich aus dem Namen des betreffenden Objekts und dem Suffix `.pgp` zusammen. Wenn das PGP Zip-Archiv mehrere Objekte enthält, wird der Dateiname aus dem Namen eines der Objekte und dem Suffix `.pgp` gebildet. Ändern Sie bei Bedarf den Dateinamen des PGP Zip-Archivs.

8. Wenn Sie die Option **Nur signieren** auswählen, klicken Sie auf **Separate Signaturen speichern**.
9. Klicken Sie auf **Weiter**. Das PGP Zip-Archiv wird erstellt.
10. Klicken Sie auf **Beenden**. Das PGP Zip-Archiv kann nun an die Empfänger gesendet werden, an deren Schlüssel das Archiv verschlüsselt wurde. Wenn sich unter den Schlüsseln, die Sie für die Verschlüsselung verwendet haben, Ihr eigener Schlüssel befindet, können Sie die Datei an einem Speicherort Ihrer Wahl ablegen.

Verschlüsselung mit Passphrasen

Verwenden Sie die Option **Passphrase** in folgenden Fällen:

- Wenn Sie ein PGP Zip-Archiv erstellen möchten, ohne Empfängerschlüssel zu verwenden (diese Option ist u. U. weniger sicher als eine Verschlüsselung mit Empfängerschlüsseln, ist jedoch noch immer sehr sicher).
- Wenn alle Empfänger PGP Desktop auf ihren Computern (Windows oder Mac OS X) installiert haben.
- Wenn Sie den Empfängern eine Passphrase mitteilen möchten.
- Wenn Sie nicht für jeden Empfänger über einen öffentlichen Schlüssel verfügen (an Ihrem Schlüsselbund oder auf einem PGP-Keyserver).

Tipp: Die Verschlüsselung mit einer Passphrase wird auch als *konventionelle Verschlüsselung* bezeichnet.

Bei der Verschlüsselung des PGP Zip-Archivs mit einer Passphrase kann eine extrem hohe Sicherheit erreicht werden, insbesondere wenn eine starke Passphrase verwendet wird. Die Verschlüsselung an Empfängerschlüssel bietet jedoch noch mehr Sicherheit. Bei der Verschlüsselung an Empfängerschlüssel benötigen die Benutzer, die im Besitz des PGP Zip-Archivs sind, zur Entschlüsselung der Datei sowohl ihre privaten Schlüssel als auch die Passphrasen. (Für jeden privaten Schlüssel eines Empfängers ist eine eigene Passphrase definiert.)

Bei der Verschlüsselung mit einer Passphrase öffnen alle Benutzer die Datei mit derselben Passphrase. Private Schlüssel sind nicht erforderlich. Alle, die im Besitz der Datei sind, mit PGP Desktop arbeiten und die Passphrase kennen, können die Datei entschlüsseln.

Achtung: Achten Sie sorgfältig darauf, dass die Passphrase für das PGP Zip-Archiv ausschließlich den Empfängern der Datei zur Verfügung gestellt wird. Wenn die Passphrase Unbefugten bekannt wird, erstellen Sie ein neues PGP Zip-Archiv mit einer anderen Passphrase. Beachten Sie jedoch, dass Sie die Original-Archivdatei und deren Inhalt nicht nachträglich neu sichern können.

Sobald die Dateien geschützt sind, senden Sie die entstandene PGP Zip-Archivdatei an die gewünschten Empfänger. Die Empfänger öffnen die PGP Zip-Archivdatei dann mit PGP Desktop. *Alle, die im Besitz der Datei und der Passphrase sind, können die PGP Zip-Archivdatei öffnen.* Alle Benutzer können auf dieselben Objekte zugreifen. Wenn Sie möchten, dass verschiedene Empfänger auf verschiedene Objekte zugreifen können, müssen Sie für jeden Empfänger ein eigenes PGP Zip-Archiv erstellen.

Achtung: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, ist die Verschlüsselung mit Passphrasen möglicherweise deaktiviert.

So verschlüsseln Sie mit einer Passphrase

1. Sofern Sie diesen Schritt noch nicht ausgeführt haben, erstellen Sie ein PGP Zip-Archiv gemäß der Anleitung unter *PGP Zip-Archive erstellen* (auf Seite 288). Folgen Sie den Anleitungen bis Schritt 6. Kehren Sie anschließend zu diesem Abschnitt zurück.
2. Wählen Sie im Fenster „Verschlüsseln“ die Option **Passphrase** aus.
3. Klicken Sie auf **Weiter**. Das Dialogfeld „Passphrase erstellen“ wird angezeigt.
4. Wenn die eingegebenen Zeichen bei der Passphraseneingabe angezeigt werden sollen, wählen Sie **Tastatureingabe anzeigen** aus.
5. Geben Sie im Feld **Passphrase** die Passphrase ein, die Sie verwenden möchten.

Die Passphrasen-Qualitätsanzeige gibt Ihnen eine Richtlinie für die Stärke der Passphrase, die Sie erstellen. Sie vergleicht den Entropiewert der eingegebenen Passphrase mit einer echten zufälligen Zeichenkette mit 128 Bit (der gleiche Entropiewert wie in einem AES128-Schlüssel). Weitere Informationen finden Sie unter *Passphrasen-Qualitätsanzeige* (siehe "Die Passphrasen-Qualitätsanzeige" auf Seite 352).

6 Geben Sie die Passphrase im Feld **Bestätigen** erneut ein.

7 Klicken Sie auf **Weiter**. Das Dialogfeld „Signieren und speichern“ wird angezeigt.

8 Auf Wunsch können Sie einen privaten Schlüssel am Schlüsselbund als Signaturschlüssel für das zu erstellende PGP Zip-Archiv angeben.

Dieser Signaturschlüssel wird verwendet, um das PGP Zip-Archiv digital zu signieren. Die Empfänger können die Herkunft des Archivs verifizieren, indem sie die digitale Signatur mit dem zugehörigen öffentlichen Schlüssel verifizieren.

- Wenn die Datei nicht signiert werden muss oder soll, wählen Sie in der Liste „Signaturschlüssel“ den Eintrag **Keiner** aus.
- Wenn Sie das PGP Zip-Archiv signieren möchten, wählen Sie Ihren Schlüssel aus der Signaturschlüsselliste aus und geben Sie die Passphrase des ausgewählten Signaturschlüssels ein (dies ist nicht die Passphrase, die zur Sicherung der Zip-Datei verwendet wird). Wenn die eingegebenen Zeichen bei der Passphraseneingabe angezeigt werden sollen, wählen Sie **Tastatureingabe anzeigen** aus.

Wenn Sie die Passphrase im Verlauf dieser Sitzung bereits mit PGP Desktop eingegeben haben, ist die Passphrase eventuell zwischengespeichert. Maßgebend sind hierbei die Einstellungen unter **Optionen**. In diesem Fall wird eine Meldung angezeigt, dass die Passphrase zwischengespeichert ist. Selbst wenn die Passphrase zwischengespeichert ist, können Sie entscheiden, die PGP Zip-Archivdatei nicht zu signieren.

9 Bestätigen Sie, dass das PGP Zip-Archiv am angegebenen Speicherort unter dem eingegebenen Dateinamen gespeichert wird. Bei Bedarf haben Sie folgende Möglichkeiten:

- Ändern Sie den Speicherort der Datei, indem Sie auf **Durchsuchen** klicken und im Windows-Dialogfeld „Datei“ einen anderen Speicherort auswählen.
- Ändern Sie den Speicherort der Datei, indem Sie manuell den Speicherort für das PGP Zip-Archiv eingeben.
- Ändern Sie den Namen der PGP Zip-Archivdatei, indem Sie ihn am Ende der Zeichenfolge des Dateispeicherorts eingeben.

Der Standarddateiname für ein PGP Zip-Archiv, das nur eine einzige Datei, ein einziges Verzeichnis oder ein einziges Laufwerk enthält, setzt sich aus dem Namen des betreffenden Objekts und dem Suffix `.pgp` zusammen. Wenn das PGP Zip-Archiv mehrere Objekte enthält, wird der Dateiname aus dem Namen eines der Objekte und dem Suffix `.pgp` gebildet. Ändern Sie bei Bedarf den Dateinamen des PGP Zip-Archivs.

10 Klicken Sie auf **Weiter**. Das PGP Zip-Archiv wird erstellt.

11 Klicken Sie auf **Beenden**. Das PGP Zip-Archiv kann jetzt an die Empfänger gesendet werden. Vergessen Sie nicht, den Empfängern die Passphrase mitzuteilen, damit diese das Archiv öffnen können.

Selbstentschlüsselnde PGP-Archive (SDA) erstellen

Verwenden Sie die Option **Selbstentschlüsselndes PGP-Archiv (SDA)** in folgenden Fällen:

- Wenn Sie ein selbstentschlüsselndes PGP Zip-Archiv erstellen möchten, ohne Empfängerschlüssel zu verwenden (diese Option ist u. U. weniger sicher als eine Verschlüsselung mit Empfängerschlüsseln, ist jedoch noch immer sehr sicher).
- Wenn Empfänger nicht über PGP Desktop verfügen und alle Empfänger Windows verwenden.
- Wenn Sie den Empfängern eine Passphrase mitteilen möchten.
- Wenn Sie nicht für jeden Empfänger über einen öffentlichen Schlüssel verfügen (an Ihrem Schlüsselbund oder auf einem PGP-Keyserver).

Ein selbstentschlüsselndes PGP-Archiv (SDA) ist ein PGP Zip-Archiv, das auf jedem beliebigen Windows-Computer geöffnet werden kann, selbst wenn PGP Desktop dort nicht installiert ist. PGP Zip SDA-Dateien sind gewöhnliche ausführbare Windows-Dateien (.exe) und können einfach per Doppelklick geöffnet werden.

PGP Zip SDA-Dateien sind etwas größer als normale PGP Zip-Archive, da für die Funktionalität zur Selbstentschlüsselung etwas zusätzlicher Speicherplatz erforderlich ist (in der Regel ca. 100 KB).

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, ist die Option zum Erstellen von selbstentschlüsselnden PGP Zip-Archiven möglicherweise deaktiviert.

Nach der Erstellung der PGP Zip-SDA-Datei können Sie das Archiv an die gewünschten Empfänger senden. *Alle, die im Besitz der Datei und der Passphrase sind, können die PGP Zip-Archivdatei öffnen.* Alle Benutzer können auf dieselben Objekte zugreifen. Wenn Sie möchten, dass verschiedene Empfänger auf verschiedene Objekte zugreifen können, müssen Sie für jeden Empfänger ein eigenes PGP Zip-Archiv erstellen.

Achtung: Achten Sie sorgfältig darauf, dass die Passphrase für das PGP Zip-SDA ausschließlich den Empfängern der Datei zur Verfügung gestellt wird. Wenn die Passphrase Unbefugten bekannt wird, erstellen Sie ein neues PGP Zip-SDA mit einer anderen Passphrase. Beachten Sie jedoch, dass Sie die Original-Archivdatei und deren Inhalt nicht nachträglich neu sichern können.

So erstellen Sie ein selbstentschlüsselndes PGP Zip-Archiv

1. Sofern Sie diesen Schritt noch nicht ausgeführt haben, erstellen Sie ein PGP Zip-Archiv gemäß der Anleitung unter *PGP Zip-Archive erstellen* (auf Seite 288). Folgen Sie den Anleitungen bis Schritt 6. Kehren Sie anschließend zu diesem Abschnitt zurück.
2. Wählen Sie im Dialogfeld „Verschlüsseln“ die Option **Selbstentschlüsselndes PGP-Archiv** aus.
3. Klicken Sie auf **Weiter**. Das Dialogfeld „Passphrase erstellen“ wird angezeigt.
4. Wenn die eingegebenen Zeichen bei der Passphraseneingabe angezeigt werden sollen, wählen Sie **Tastatureingabe anzeigen** aus.
5. Geben Sie im Feld **Passphrase** die Passphrase ein, die Sie verwenden möchten.

   Die Passphrasen-Qualitätsanzeige gibt Ihnen eine Richtlinie für die Stärke der Passphrase, die Sie erstellen. Sie vergleicht den Entropiewert der eingegebenen Passphrase mit einer echten zufälligen Zeichenkette mit 128 Bit (der gleiche Entropiewert wie in einem AES128-Schlüssel). Weitere Informationen finden Sie unter *Passphrasen-Qualitätsanzeige* (siehe "Die Passphrasen-Qualitätsanzeige" auf Seite 352).
6. Geben Sie die Passphrase im Feld **Bestätigen** erneut ein.
7. Klicken Sie auf **Weiter**.
8. Bestätigen Sie, dass das PGP Zip-Archiv am angegebenen Speicherort unter dem eingegebenen Dateinamen gespeichert wird. Bei Bedarf haben Sie folgende Möglichkeiten:
   - Ändern Sie den Speicherort der Datei, indem Sie auf **Durchsuchen** klicken und im Windows-Dialogfeld „Datei“ einen anderen Speicherort auswählen.
   - Ändern Sie den Speicherort der Datei, indem Sie manuell den Speicherort für das PGP Zip-Archiv eingeben.
   - Ändern Sie den Namen der PGP Zip-Archivdatei, indem Sie ihn am Ende der Zeichenfolge des Dateispeicherorts eingeben.

   Der Standarddateiname für ein PGP Zip-Archiv, das nur eine einzige Datei, ein einziges Verzeichnis oder ein einziges Laufwerk enthält, setzt sich aus dem Namen des betreffenden Objekts und dem Suffix `.pgp` zusammen. Wenn das PGP Zip-Archiv mehrere Objekte enthält, wird der Dateiname aus dem Namen eines der Objekte und dem Suffix `.pgp` gebildet. Ändern Sie bei Bedarf den Dateinamen des PGP Zip-Archivs.

9 Klicken Sie auf **Weiter**. Das PGP Zip-SDA wird erstellt.

10 Klicken Sie auf **Beenden**. Das PGP Zip-SDA kann jetzt an die Empfänger gesendet werden.

Ein Archiv nur mit Signatur erstellen

Verwenden Sie **Nur signieren** in folgenden Fällen:

- Wenn Sie die Dateien nicht verschlüsseln (und damit den Empfängern keine Passphrase mitteilen) müssen.
- Wenn Sie eine Signaturdatei erstellen möchten, mit der die Empfänger bestätigen können, dass das erhaltene PGP Zip-Archiv tatsächlich von Ihnen stammt. Jede Datei wird einzeln verarbeitet und mit einer separaten Signatur versehen.
- Wenn alle Empfänger PGP Desktop auf ihren Computern (Windows oder Mac OS X) installiert haben.
- Wenn Sie garantieren möchten, dass Sie die Datei geschickt haben, und wenn Sie Ihrem Empfänger versichern möchten, dass die Datei während der Übertragung nicht geändert wurde.

In Situationen, in denen Sie die Datei(en) für die Empfänger nicht verschlüsseln müssen, können Sie die Option „Nur signieren“ wählen. Anstatt die Dateien zu verschlüsseln und in einem PGP Zip-Archiv zu komprimieren, löst diese Option nur die Komprimierung aus.

So führen Sie eine Verschlüsselung mit der Option „Nur signieren“ durch

1 Sofern Sie diesen Schritt noch nicht ausgeführt haben, erstellen Sie ein PGP Zip-Archiv gemäß der Anleitung unter *PGP Zip-Archive erstellen* (auf Seite 288). Folgen Sie den Anleitungen bis Schritt 6. Kehren Sie anschließend zu diesem Abschnitt zurück.

Hinweis: Wenn Sie wählen, die Dateien zu komprimieren und zu signieren, wird die Option **Nach Abschluss Originaldateien an PGP Shredder senden** ignoriert, selbst wenn Sie sie ausgewählt haben.

2 Wählen Sie im Dialogfeld „Verschlüsseln“ die Option **Nur signieren** aus.

3 Klicken Sie auf **Weiter**. Der Bildschirm **Signieren und speichern** wird angezeigt.

4 Geben Sie einen privaten Schlüssel am Schlüsselbund als Signaturschlüssel für das zu erstellende PGP Zip-Archiv an.

Dieser Signaturschlüssel wird verwendet, um das PGP Zip-Archiv digital zu signieren. Die Empfänger können die Herkunft des Archivs verifizieren, indem sie die digitale Signatur mit dem zugehörigen öffentlichen Schlüssel verifizieren.

- Wenn die Datei nicht signiert werden muss oder soll, wählen Sie in der Liste „Signaturschlüssel“ den Eintrag **Keiner** aus.
- Wenn Sie das PGP Zip-Archiv signieren möchten, wählen Sie Ihren Schlüssel aus der Signaturschlüsselliste aus und geben Sie die Passphrase des ausgewählten Signaturschlüssels ein (dies ist nicht die Passphrase, die zur Sicherung der Zip-Datei verwendet wird). Wenn die eingegebenen Zeichen bei der Passphraseneingabe angezeigt werden sollen, wählen Sie **Tastatureingabe anzeigen** aus.

Wenn Sie die Passphrase im Verlauf dieser Sitzung bereits mit PGP Desktop eingegeben haben, ist die Passphrase eventuell zwischengespeichert. Maßgebend sind hierbei die Einstellungen unter **Optionen**. In diesem Fall wird eine Meldung angezeigt, dass die Passphrase zwischengespeichert ist. Selbst wenn die Passphrase zwischengespeichert ist, können Sie entscheiden, die PGP Zip-Archivdatei nicht zu signieren.

5 Vergewissern Sie sich, dass das PGP Zip-Archiv am angegebenen Speicherort erstellt wird. Bei Bedarf haben Sie folgende Möglichkeiten:

- Ändern Sie den Speicherort der Datei, indem Sie auf **Durchsuchen** klicken und im Windows-Dialogfeld „Datei“ einen anderen Speicherort auswählen.
- Ändern Sie den Speicherort der Datei, indem Sie manuell den Speicherort für das PGP Zip-Archiv eingeben.

Der Standarddateiname für ein nur signiertes PGP Zip-Archiv setzt sich aus dem Namen des betreffenden Objekts und dem Suffix `.sig` zusammen.

6 Wenn zusätzlich zum PGP Zip-Archiv eine separate Signaturdatei erstellt werden soll, klicken Sie auf **Separate Signaturen speichern**.

7 Klicken Sie auf **Weiter**. Das nur signierte PGP Zip-Archiv wird erstellt.

8 Klicken Sie auf **Beenden**.

PGP Zip-Archive öffnen

PGP Desktop muss auf dem Computer installiert sein, damit ein PGP Zip-Archiv geöffnet werden kann.

So öffnen Sie ein PGP Zip-Archiv

1 Doppelklicken Sie auf die PGP Zip-Archivdatei (diese hat die Dateiendung `.pgp`).

- Wenn das PGP Zip-Archiv mit einem Schlüssel gesichert wurde, wird das Dialogfeld „PGP-Passphrase für aufgelisteten Schlüssel eingeben“ angezeigt.

- Wenn das PGP Zip-Archiv mit einem Schlüssel gesichert wurde, wird das Dialogfeld „PGP-Passphrase eingeben“ angezeigt.

PGP Desktop zeigt den Inhalt des PGP Zip-Archivs an. (Wenn PGP Desktop nicht geöffnet ist, wird die Anwendung mit dem aktiven PGP Zip-Objekt geöffnet.)

2 Gehen Sie folgendermaßen vor, um Objekte zu extrahieren:

- Wenn Sie ein einzelnes Objekt extrahieren möchten, klicken Sie mit der rechten Maustaste auf das Objekt und wählen Sie im Kontextmenü die Option **Extrahieren** aus.
- Wenn Sie mehrere Objekte extrahieren möchten, wählen Sie die Objekte aus, klicken Sie mit der rechten Maustaste auf eines der Objekte und wählen Sie im Kontextmenü die Option **Extrahieren** aus.

Das Dialogfeld „Ordner suchen“ wird angezeigt.

3 Suchen Sie den Ordner, in den die Dateien extrahiert werden sollen, und klicken Sie auf „OK“. Wenn Sie einen neuen Ordner erstellen möchten, klicken Sie auf **Neuer Ordner**. Die Dateien werden an den von Ihnen festgelegten Speicherort extrahiert.

Wenn Sie die entschlüsselten Dateien aus dem PGP Zip-Archiv an denselben Speicherort extrahieren, von dem sie komprimiert wurden, werden die Originaldateien überschrieben. Um ein versehentliches Überschreiben zu vermeiden, werden Sie bei jeder Datei aufgefordert zu prüfen, ob Sie die vorhandene Datei tatsächlich überschreiben möchten.

PGP Zip-SDAs öffnen

Zum Öffnen eines PGP Zip-SDA muss PGP Desktop nicht installiert sein.

So öffnen Sie ein PGP Zip-SDA

1 Doppelklicken Sie auf die PGP Zip-SDA-Datei (diese hat die Dateiendung `.exe`). Das Dialogfeld „Selbstentschlüsselndes PGP-Archiv – Passphrase eingeben“ wird angezeigt.

2 Vergewissern Sie sich, dass die Ausgabe an den gewünschten Speicherort extrahiert werden soll. Ist dies nicht der Fall, klicken Sie auf **Durchsuchen**, um den Speicherort zu korrigieren, oder geben Sie ihn in das Feld ein.

Hinweis: Wenn Sie die entschlüsselten Dateien aus dem PGP-Zip-SDA an denselben Speicherort extrahieren, von dem sie komprimiert wurden, werden die Originaldateien überschrieben. Damit dies verhindert wird, werden Sie bei jeder Datei aufgefordert, einen anderen Speicherort auszuwählen. Sie können auch einen anderen Dateinamen eingeben. Wenn Sie auf **Speichern** klicken, ohne einen anderen Speicherort auszuwählen, wird eine Warnung angezeigt. Wenn Sie diese Warnung umgehen, wird die Originaldatei mit der Datei aus dem PGP Zip-SDA überschrieben.

3 Geben Sie die Passphrase für das PGP Zip-SDA ein und klicken Sie auf **OK**. Das PGP Zip-SDA wird entschlüsselt.

PGP Zip-Archive bearbeiten

PGP Zip-Archive sind nicht statisch. Die folgenden Vorgänge sind jederzeit möglich:

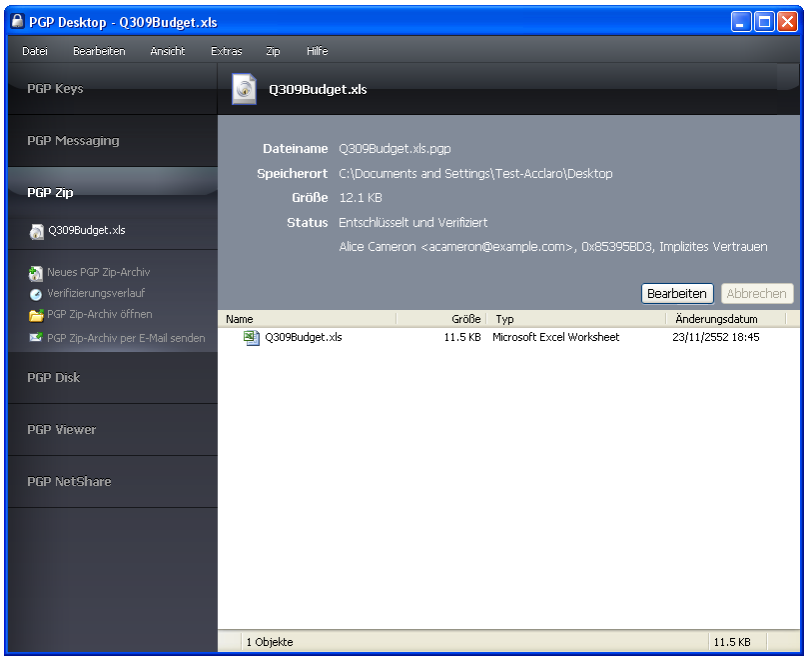
- Dateien aus dem Archiv extrahieren
- Dateien in das Archiv einfügen
- Einstellungen des Archivs bearbeiten

So bearbeiten Sie ein PGP Zip-Archiv

1 Klicken Sie in PGP Desktop auf das Bedienfeld „PGP Zip“. Das Bedienfeld „PGP Zip“ wird markiert.

2 Klicken Sie im oberen Bereich des Bedienfelds „PGP Zip“ in der Liste der PGP Zip-Archive auf das Archiv, das Sie bearbeiten möchten. Die Einstellungen für das Archiv und die Dateien bzw. Ordner im Archiv werden angezeigt.

Wenn das PGP Zip-Archiv, das Sie öffnen möchten, nicht in der Liste aufgeführt ist, klicken Sie auf **PGP Zip-Archiv öffnen**, wechseln Sie zur gewünschten Datei mit der Endung `.pgp`, wählen Sie sie aus und klicken Sie auf **Öffnen**.



3 Wenn Sie die Einstellungen des PGP Zip-Archivs bearbeiten möchten, klicken Sie auf **Bearbeiten** und nehmen Sie die gewünschten Änderungen vor:

- **Wenn Sie dem PGP Zip-Archiv weitere Dateien hinzufügen möchten**, klicken Sie im Bedienfeld „PGP Zip“ auf **Dateien hinzufügen**, markieren die gewünschten Dateien und klicken dann auf **Öffnen**. Die Dateien werden dem Archiv hinzugefügt.
- **Wenn Sie dem Archiv einen Ordner hinzufügen und Dateien in diesen Ordner einfügen möchten**, klicken Sie im Bedienfeld „PGP Zip“ auf **Neuer Ordner** und geben Sie einen aussagekräftigen Namen für den neuen Ordner ein (wenn gewünscht). Wählen Sie den neuen Ordner aus, klicken Sie im Bedienfeld „PGP Zip“ auf **Dateien hinzufügen**, wählen Sie die Dateien aus, die dem Ordner hinzugefügt werden sollen, und klicken Sie auf **Öffnen**. Die Dateien werden dem Archiv im angegebenen Ordner hinzugefügt.
- **Wenn Sie eine Datei aus einem Archiv extrahieren möchten**, klicken Sie mit der rechten Maustaste auf die gewünschte Datei, wählen im Kontextmenü die Option **Extrahieren** aus, geben einen Speicherort für die Datei an und klicken auf **OK**. Am angegebenen Speicherort wird eine Kopie der Datei erstellt. Das Original verbleibt im PGP Zip-Archiv.

- **Wenn Sie eine Datei oder einen Ordner aus einem Archiv löschen möchten**, wählen Sie die gewünschten Objekte aus und drücken Sie auf der Tastatur die Taste **Entfernen**. Sie können auch **Bearbeiten > Löschen** auswählen. Die angegebenen Objekte werden gelöscht.
- **Wenn Sie die an einem PGP Zip-Archiv vorgenommenen Änderungen speichern möchten**, klicken Sie in der rechten oberen Ecke auf **Speichern** oder im Bedienfeld „PGP Zip“ auf **PGP Zip-Archiv speichern**. Geben Sie einen Speicherort und einen Namen an. Wenn der gewählte Name am Speicherort bereits vorhanden ist, werden Sie gefragt, ob die vorhandene Datei überschrieben werden soll. Geben Sie die Passphrase ein, mit der das Archiv geschützt ist, und klicken Sie auf **OK**.
- **Wenn Sie den Signaturschlüssel ändern möchten**, wählen Sie im Bedienfeld „PGP Zip“ die gewünschte PGP Zip-Datei aus. Klicken Sie auf **Bearbeiten** und wählen Sie einen neuen **Signaturschlüssel** aus. Klicken Sie am Ende auf **Speichern**.
- **Wenn Sie die Verschlüsselungsmethode ändern möchten** (Schlüssel oder konventionell), wählen Sie im Bedienfeld „PGP Zip“ die gewünschte PGP Zip-Datei aus. Klicken Sie auf **Bearbeiten** und wählen Sie die Verschlüsselungsmethode (**Schlüssel** oder **Konventionell**) aus. Klicken Sie am Ende auf **Speichern**.
- **Wenn Sie dem PGP Zip-Archiv Empfänger hinzufügen möchten**, wählen Sie die gewünschte PGP Zip-Datei im Bedienfeld „PGP Zip“ aus, klicken auf **Bearbeiten** und dann auf **Empfänger hinzufügen**. Wählen Sie im Dialogfeld „Empfänger hinzufügen“ die gewünschten Empfänger aus und klicken Sie auf **OK**. Klicken Sie am Ende auf **Speichern**.
- **Wenn Sie Empfänger aus dem Archiv löschen möchten**, wählen Sie die gewünschte PGP Zip-Datei im Bedienfeld „PGP Zip“ aus, klicken auf **Bearbeiten**, wählen den gewünschten Empfänger aus und klicken auf **Empfänger löschen**. Klicken Sie am Ende auf **Speichern**.

4 Wenn Sie mit der Bearbeitung fertig sind, klicken Sie auf **Speichern. Sie können das vorherige PGP Zip-Archiv durch das veränderte Archiv ersetzen oder das veränderte Archiv unter einem neuen Namen speichern.**

Signierte PGP Zip-Archive verifizieren

Wenn Sie ein signiertes PGP Zip-Archiv erhalten, sollten Sie die Signatur prüfen, damit Sie deren Herkunft kennen und sichergehen können, dass das Archiv nicht verfälscht wurde, bevor Sie es erhalten haben.

So verifizieren Sie ein PGP Zip-Archiv

1. Klicken Sie auf das Bedienfeld „PGP Zip“ und dann auf **PGP Zip-Archiv öffnen**. Das Dialogfeld „Öffnen“ wird angezeigt.
2. Wechseln Sie zu der signierten PGP-Datei, die Sie verifizieren möchten, wählen Sie sie aus und klicken Sie auf **Öffnen**.

   Wenn die Nachricht nicht nur signiert, sondern auch verschlüsselt wurde, werden Sie aufgefordert, die Passphrase Ihres privaten Schlüssels einzugeben bzw. des privaten Schlüssels, der dem öffentlichen Schlüssel entspricht, an den die Nachricht verschlüsselt wurde.

   Wenn sich der private Schlüssel nicht an Ihrem Schlüsselbund befindet, wird von PGP Desktop ein Hinweis angezeigt, dass die Nachricht nicht entschlüsselt werden kann. Dies bedeutet leider auch, dass Sie das Archiv nicht verifizieren können. Klicken Sie auf **Abbrechen, um die Verifizierung abzubrechen.**
3. Geben Sie die Passphrase des privaten Schlüssels ein und klicken Sie auf **OK**.

   Hinweis: Wenn die Passphrase des privaten Schlüssels zwischengespeichert wurde, werden Sie nicht zur Eingabe der Passphrase aufgefordert.

   Der Inhalt des Archivs wird an demselben Speicherort wie das PGP Zip-Archiv abgelegt. Im Bildschirm „Verifizierungsverlauf“ finden Sie Informationen zu dem Archiv, das Sie verifizieren.
4. Wenn Sie die Liste der verifizierten Archive löschen möchten, klicken Sie auf **Verifizierungsverlauf löschen**. Alle Einträge des Bildschirms „Verifizierungsverlauf“ werden entfernt.

15 Dateien mit PGP Shredder sicher löschen

Falls Sie vertrauliche Dateien vollständig vernichten möchten, ohne Fragmente der Daten zurückzulassen, verwenden Sie das Dienstprogramm PGP Shredder.

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung verwenden, hat Ihr PGP Universal Server-Administrator ggf. bestimmte Funktionen deaktiviert. Ist eine Funktion deaktiviert, wird das Bedienelement auf der linken Seite nicht angezeigt und das Menü oder andere auf diese Funktion zutreffenden Optionen sind nicht verfügbar. Die in diesem Handbuch enthaltenen Abbildungen entsprechen der Standardinstallation, bei der alle Funktionen aktiviert sind. Wenn Ihr PGP Universal Server-Administrator diese Funktion deaktiviert hat, ist dieser Abschnitt für Sie nicht relevant.

In diesem Kapitel

Dateien und Ordner mit PGP Shredder sicher und endgültig löschen ..305
PGP-Assistent zum sicheren Löschen von freiem Speicherplatz 308

Dateien und Ordner mit PGP Shredder sicher und endgültig löschen

Wenn Sie vertrauliche Dateien oder Ordner vollständig vernichten möchten, verwenden Sie hierzu PGP Shredder. Wenn Sie Dateien oder Ordner mit PGP Shredder löschen, bleiben keine Spuren zurück.

PGP Shredder überschreibt die Daten mit Zufallstext. Dieser Vorgang wird in mehreren *Durchgängen* ausgeführt. Sie können die Anzahl der Durchgänge der PGP Shredder-Funktion festlegen, indem Sie im Bildschirm „Einstellungen“ den Bereich „Laufwerk“ öffnen. Weitere Informationen zum Einstellen von Optionen und Einstellungen finden Sie im Abschnitt zu Laufwerksoptionen und -einstellungen unter *Laufwerksoptionen* (auf Seite 342).

Das sichere Löschen kann einige Zeit in Anspruch nehmen. Die Dauer hängt u. a. von der Anzahl der festgelegten Durchgänge, der Prozessorgeschwindigkeit sowie der Anzahl der ausgeführten anderen Anwendungen ab.

Hinweis: Bei drei Durchgängen überschreitet PGP Shredder bereits die Mindestvorschriften der Datenträgerrichtlinien des US-Verteidigungsministeriums, Norm 5220.22-M. Obwohl eine größere Anzahl von Durchgängen zulässig ist, sind für moderne Diskhardware nicht mehr als zwei Durchgänge erforderlich. Die Sicherheit erhöht sich weiter bis zu ungefähr 28 Durchgängen. Mit PGP Shredder können bis zu 49 Durchgänge ausgeführt werden, jedoch ist dabei zu beachten, dass der erforderliche Zeitaufwand mit der Anzahl der Durchgänge zunimmt.

PGP Shredder kann auf verschiedene Weise eingesetzt werden:

- Verwenden Sie das PGP Shredder-Symbol auf dem Desktop (das bei der Installation von PGP Desktop dort abgelegt wurde).
- Klicken Sie auf **Extras > Dateien sicher löschen** und wechseln Sie zu den Dateien oder Ordnern, die Sie sicher löschen möchten.
- Verwenden Sie die Kontextmenüs von Windows Explorer (klicken Sie mit der rechten Maustaste auf die Datei und wählen Sie **PGP Desktop > PGP Shred [Dateiname]** aus).

Folgende Objekte werden nicht von PGP Shredder gelöscht:

- Windows-Systemdateien oder schreibgeschützte Dateien

  Beachten Sie, dass die Datei Thumbs.db, die bei der Anzeige von Miniaturbildern in Windows Explorer erstellt wird, einen Sonderfall darstellt und sicher gelöscht werden kann, obwohl die Datei das Systemattribut aufweist

  WebDav- oder Sharepoint-Dateien Lokale Dateien und freigegebene CIFS Dateien können gelöscht werden.
- Verzeichnisse mit Dateien, die nicht gelöscht werden können

Sie können PGP Desktop auch verwenden, um mit dem PGP-Assistenten zum sicheren Löschen von freiem Speicherplatz freien Festplattenspeicher zu löschen, der Daten von früher gelöschten Dateien und Anwendungen enthalten könnte.

Es ist besonders wichtig, den PGP-Assistenten zum sicheren Löschen von freiem Speicherplatz auf Dateisystemen mit Journalerstellung, z. B. NTFS, zu verwenden, da diese Dateisysteme in einem Dateisystemjournal eine Kopie aller Daten ablegen, die auf die Festplatte geschrieben wurden. Dies ist beim Wiederherstellen der Festplatte bei Schäden hilfreich, erfordert aber zusätzliche Arbeit beim Entfernen vertraulicher Daten. Durch das sichere Löschen einer Datei werden Journaleinträge, die möglicherweise erstellt wurden, nicht entfernt. Insbesondere NTFS kann kleine Dateien (unter 1 KB) in internen Datenstrukturen speichern, die ohne den PGP-Assistenten zum sicheren Löschen von freiem Speicherplatz mit der Option **Interne NTFS-Datenstrukturen sicher löschen** nicht vollständig gelöscht werden können.

Tipp: Daten können u. U. auch an anderen Speicherorten abgelegt sein, z. B. in temporären Dateien. Aus diesem Grund sollten Sie PGP Whole Disk Encryption verwenden, um alle Daten auf dem System zu schützen.

Dateien mithilfe des PGP Shredder-Symbols auf Ihrem Desktop dauerhaft löschen

▸ **So vernichten Sie Dateien mithilfe des PGP Shredder-Symbols auf Ihrem Desktop**

1. Ziehen Sie die Dateien/Ordner, die Sie sicher löschen möchten, auf das PGP Shredder-Symbol. Sie werden in einem Bestätigungsdialogfeld aufgefordert, das sichere Löschen der aufgeführten Dateien und/oder Ordner zu bestätigen.
2. Klicken Sie auf **Ja.** Die Dateien werden sicher vom System gelöscht.

Dateien über PGP Desktop sicher löschen

▸ **So können Sie Dateien in PGP Desktop sicher löschen**

1. Klicken Sie im Hauptanwendungsfenster von PGP Desktop auf **Extras > Dateien sicher löschen**. Das Dialogfeld „Öffnen“ wird angezeigt.
2. Wählen Sie die Dateien aus, die Sie sicher löschen möchten, und klicken Sie auf **Öffnen.** Sie werden in einem Bestätigungsdialogfeld aufgefordert, das sichere Löschen der aufgeführten Dateien und/oder Ordner zu bestätigen.
3. Klicken Sie auf **Ja.** Die Dateien werden sicher vom System gelöscht.

Dateien aus Windows Explorer sicher löschen

▸ **So löschen Sie sicher Dateien mit dem Kontextmenü von Windows Explorer**

1. Klicken Sie in Windows Explorer mit der rechten Maustaste auf die Dateien bzw. Ordner, die Sie sicher löschen möchten. Sie werden in einem Bestätigungsdialogfeld aufgefordert, das sichere Löschen der aufgeführten Dateien und/oder Ordner zu bestätigen.
2. Klicken Sie auf **Ja.** Die Dateien werden sicher vom System gelöscht.

PGP-Assistent zum sicheren Löschen von freiem Speicherplatz

So wird freier Speicherplatz auf Laufwerken sicher gelöscht

1. Öffnen Sie PGP Desktop und wählen Sie **Extras** > **Freien PGP-Speicherplatz sicher löschen** aus. Der Einführungsbildschirm des PGP-Assistenten zum sicheren Löschen von freiem Speicherplatz wird angezeigt.
2. Lesen Sie die Informationen und klicken Sie auf **Weiter**.Das Dialogfeld „Informationen werden gesammelt“ wird angezeigt.
3. Wählen Sie im Feld **Laufwerk sicher löschen** das Laufwerk aus, das Sie sicher löschen möchten, sowie die Anzahl der **Durchgänge**, die die Funktion „Freien Speicherplatz sicher löschen“ ausführen soll. Obgleich drei Durchgänge mit PGP Shred ausreichend sind, um Daten sicher zu löschen, können Sie bis zu 49 Durchgänge einplanen. Folgende Richtlinien werden für die Anzahl der Durchgänge empfohlen:
   - 3 Durchgänge für den persönlichen Gebrauch
   - 10 Durchgänge für den kommerziellen Gebrauch
   - 18 Durchgänge für den militärischen Gebrauch
   - 26 Durchgänge für optimale Sicherheit
4. Wählen Sie, ob interne NTFS-Datenstrukturen sicher gelöscht werden sollen. Diese Option ist nicht auf allen Systemen verfügbar.

   Achtung: Falls es sich bei der ausgewählten Partition *nicht* um die Startpartition handelt, können Sie eine intensive sichere Löschung durchführen, um interne NTFS-Datenstrukturen zu überschreiben, die Datenreste enthalten können. Die Partition wird bei diesem Verfahren vollständig ausgefüllt. Daher *sollten Sie das Laufwerk während des sicheren Löschens von freiem Speicherplatz für keine anderen Operationen verwenden*. Einige dieser Strukturen werden im Allgemeinen nicht als freier Speicherplatz auf dem Laufwerk angesehen, aber die Techniken, die von dieser Option angewendet werden, bewirken, das sie sicher gelöscht werden. Diese Option erhöht nicht das Risiko, dass die Festplatte durch das sichere Löschen auf irgendeine Weise beeinträchtigt wird.
5. Klicken Sie auf **Weiter**.Das Dialogfeld „Sicheres Löschen durchführen“ wird angezeigt mit statistischen Informationen zum ausgewählten Laufwerk bzw. zum ausgewählten Volume.
6. Führen Sie einen der folgenden Schritte aus:

- Wenn Sie sofort mit dem sicheren Löschen beginnen möchten, klicken Sie auf **Sicheres Löschen starten**.Der PGP-Assistent zum sicheren Löschen von freiem Speicherplatz sucht nach übrig gebliebenen Fragmenten und löscht diese dann sicher vom angegebenen Laufwerk bzw. vom angegebenen Datenträger.

  Wenn die Sitzung beendet ist, wird eine Nachricht am unteren Rand des Bildschirms „Sicheres Löschen durchführen“ angezeigt, dass das ausgewählte Laufwerk sicher gelöscht wurde.

- Wenn Sie das sichere Löschen von freiem Speicherplatz zeitlich planen möchten, klicken Sie auf **Planen**. In einer Meldung werden Sie darauf hingewiesen, dass für das Planen von Operationen der PGP-Funktion „Freien Speicherplatz sicher löschen“ der Windows-Taskplaner verwendet wird und dass Sie zum Ausführen dieses Auftrags ein Windows-Kennwort benötigen.

  Klicken Sie zum Planen des Auftrags auf **OK**, geben Sie das Windows-Kennwort im Dialogfeld „Bestätigte PGP-Passphrase eingeben“ ein und geben Sie die zum Planen erforderlichen Informationen ein.

  Wenn Sie den Auftrag abbrechen und zum Dialogfeld „Sicheres Löschen durchführen“ zurückkehren möchten, klicken Sie auf **Abbrechen**.

7 Klicken Sie auf **Weiter**.Der Abschlussbildschirm wird angezeigt.

8 Klicken Sie auf **Fertig stellen**.

Sicheres Löschen des freien Speicherplatzes planen

Verwenden Sie den Windows-Taskplaner, um den freien Speicherplatz auf dem System in bestimmten Abständen sicher zu löschen.

So planen Sie das sichere Löschen des freien Speicherplatzes

1 Führen Sie die Schritte unter *PGP-Assistent zum sicheren Löschen von freiem Speicherplatz* (auf Seite 308) aus, bis das Dialogfeld „Sicheres Löschen durchführen“ angezeigt wird.

2 Klicken Sie auf **Planen**.

3 In einer Meldung werden Sie darauf hingewiesen, dass für das Planen von Operationen der PGP-Funktion „Freien Speicherplatz sicher löschen“ der Windows-Taskplaner verwendet wird und dass Sie zum Ausführen dieses Auftrags ein Windows-Kennwort benötigen. Klicken Sie zum Fortfahren auf **OK**. Das Dialogfeld „Bestätigte PGP-Passphrase eingeben“ wird angezeigt.

4 Geben Sie im ersten Feld das Windows-Kennwort ein, geben Sie es im zweiten Feld zur Bestätigung erneut ein und klicken Sie auf **OK**.Das Dialogfeld „Windows-Taskplaner“ wird angezeigt.

5 Geben Sie im Feld **Task planen** an, wie oft der Auftrag ausgeführt werden soll:

- **Täglich**:Diese Option führt den Task einmal zum angegebenen Zeitpunkt an den angegebenen Tagen aus. Klicken Sie auf **OK**, um das Dialogfeld zu schließen, und geben Sie in das Textfeld „Startzeit" den Zeitpunkt ein, an dem der Task jeden Tag ausgeführt werden soll.
- **Wöchentlich**:Diese Option führt den Task auf wöchentlicher Basis zum angegebenen Datum und Zeitpunkt aus. Geben Sie die Anzahl der Wochen zwischen den Löschoperationen in das vorgesehene Textfeld ein und wählen Sie einen Tag in der Liste „Auftrag wöchentlich ausführen" aus.
- **Monatlich**:Diese Option führt den Task einmal monatlich am angegebenen Tag und Zeitpunkt aus. Geben Sie den Zeitpunkt in das vorgesehen Textfeld ein und geben Sie dann den Tag des Monats ein, an dem der Task ausgeführt werden soll. Klicken Sie auf **Monate auswählen**, um anzugeben, in welchen Monaten der Task ausgeführt werden soll.
- **Einmalig**:Diese Option führt den Task genau einmal am angegebenen Datum und Zeitpunkt aus. Geben Sie den Zeitpunkt in das vorgesehene Textfeld ein und wählen Sie einen Monat und ein Datum aus den Listen im Textfeld zum einmaligen Ausführen aus.
- **Beim Systemstart**:Diese Option führt den Task nur beim Systemstart aus.
- **Beim Anmelden**: Diese Option führt den Task aus, wenn Sie sich beim Computer anmelden.
- **Im Leerlauf**:Diese Option führt den Task aus, wenn das System während der Zeitdauer im Leerlauf ist, die Sie im Textfeld „Minuten" angeben.

6 Geben Sie im Feld **Startzeit** die Uhrzeit an, zu der die Ausführung des Tasks starten soll.

7 Geben Sie im Feld „Aufgabe täglich ausführen" an, wie oft der Auftrag ausgeführt werden soll.

8 Klicken Sie auf **Erweitert**, um ein Dialogfeld zu öffnen, in dem Sie zusätzliche Optionen auswählen können, z. B. das Startdatum, das Enddatum und die Dauer des Tasks.

9 Klicken Sie auf **OK**.Ein Bestätigungsdialogfeld wird angezeigt.

Der neue Task für PGP-Ordner oder freien Speicherplatz ist jetzt geplant. Verwenden Sie den Windows-Taskplaner zum Bearbeiten oder Löschen des PGP-Tasks.

16 Schlüssel auf Smartcards und Token speichern

Verwenden Sie PGP Desktop, um ein PGP-Schlüsselpaar auf einer Smartcard oder einem Token zu erstellen oder ein PGP-Schlüsselpaar auf eine Smartcard oder ein Token zu kopieren. Beide Optionen sorgen für ein zusätzliches Sicherheitsniveau, da Sie Ihr PGP-Schlüsselpaar auf der Smartcard oder dem Token immer mitführen können, anstatt es auf dem System zu belassen: Ein PGP-Schlüsselpaar auf einer Smartcard oder einem Token ist weniger gefährdet als dasselbe Schlüsselpaar, das auf dem Computer gespeichert ist, da Sie die Smartcard bzw. das Token bei sich tragen können. In diesem Abschnitt wird die Verwendung von Smartcards mit PGP Desktop erläutert.

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung verwenden, hat Ihr PGP Universal Server-Administrator ggf. bestimmte Funktionen deaktiviert. Ist eine Funktion deaktiviert, wird das Bedienelement auf der linken Seite nicht angezeigt und das Menü oder andere auf diese Funktion zutreffenden Optionen sind nicht verfügbar. Die in diesem Handbuch enthaltenen Abbildungen entsprechen der Standardinstallation, bei der alle Funktionen aktiviert sind. Wenn Ihr PGP Universal Server-Administrator diese Funktion deaktiviert hat, ist dieser Abschnitt für Sie nicht relevant.

In diesem Kapitel

Informationen zu Smartcards und Token 312
Smartcard-Eigenschaften untersuchen 315
Ein PGP-Schlüsselpaar auf einer Smartcard generieren 316
Öffentliche Schlüssel von Smartcards auf Schlüsselbunde kopieren 318
Schlüsselpaare vom Schlüsselbund auf eine Smartcard kopieren 319
Schlüssel von der Smartcard sicher löschen 320
Mehrere Smartcards verwenden 321
Sonder-Token 322

Informationen zu Smartcards und Token

Damit Sie PGP Desktop mit einer Smartcard oder einem Token eines bestimmten Anbieters verwenden können, müssen Sie über ein kompatibles Smartcard-Lesegerät verfügen (falls Sie eine Smartcard verwenden) und die entsprechenden Software-Treiber auf dem System installiert haben (sowohl für Smartcards als auch Token). Die Treiber *müssen* die PKCS-11-Bibliothek (Cryptographic Token Interface Standard) enthalten.

Die PGP Corporation empfiehlt Ihnen dringend, Software-Treiber von dem Anbieter zu verwenden, der auch die Smartcard oder das Token herstellt.

PGP Desktop erkennt und unterstützt eine Vielzahl von Smartcards, darunter Smartcards von Athena, AET SafeSign, Axalto (früher Schlumberger), SafeNet (früher Rainbow), Aladdin und GemPlus. PGP Desktop ist auch mit Common Access Cards des US-amerikanischen Verteidigungsministeriums Department of Defense mit dem ActivCard Gold 2.0-Profil kompatibel.

Zusätzlich zu diesen Anbietern erkennt und arbeitet PGP Desktop mit Smartcards von Anbietern, deren Software-Treiber eine auf Standards basierte PKCS-11-Bibliothek enthält. Wenn die PKCS-11-Bibliothek eines Anbieters auf Ihrem System installiert ist und mit anderen PKCS-11-Anwendungen wie z. B. Mozilla Firefox oder Thunderbird funktioniert, ist die Wahrscheinlichkeit groß, dass PGP Desktop Smartcards von diesem Anbieter erkennt und damit arbeiten kann.

Wenn Sie ein PGP-Schlüsselpaar auf einer Smartcard erstellen und speichern, verwenden Sie keine Passphrase, sondern die PIN der Smartcard zum Zugriff auf den privaten Schlüssel. Falls Sie eine Smartcard besitzen, die für ihre eigene Authentifizierung sorgt (beispielsweise auf ihrer eigenen Tastatur oder über ein biometrisches Gerät), kann diese mit PGP Desktop verwendet werden. Wenn in PGP Desktop ein Passphrasen-Dialogfeld angezeigt wird, geben Sie keine Passphrase ein, sondern klicken Sie auf „OK“. Das Gerät wird dann seine eigene Authentifizierungsmethode anzeigen.

Hinweis: Der private Abschnitt des Schlüsselpaars, der auf einer Smartcard erstellt wird, bleibt stets auf dem Gerät, d. h. er kann nicht exportiert werden. Entschlüsselung und Signierung finden direkt auf dem Gerät statt. Wenn Sie ein Schlüsselpaar auf dem Computer und nicht auf der Smartcard erstellen und das Schlüsselpaar dann auf die Smartcard kopieren, während das Schlüsselpaar auf dem Computer verbleibt, können Sie weiterhin den privaten Abschnitt des Schlüsselpaars vom Computer kopieren.

CAC-Cards des US-Verteidigungsministeriums

Department of Defense Common Access Cards (CACs) unterscheiden sich in ihrer Funktionsweise von anderen Smartcards. Sie sind schreibgeschützt und enthalten zwei separate Zertifikate: eines zum Signieren und das andere zum Verschlüsseln. PGP Desktop filtert die beiden Zertifikate anhand des Nutzungszwecks. Wenn Sie z. B. aufgefordert werden, einen Schlüssel zum Signieren einer Datei auszuwählen, wird nur das Signierzertifikat der CAC angezeigt.

JavaCards

Axalto-Smartcards sind JavaCards. Auf der Karte wird ein kleines Java-Modul ausgeführt, das Java-Applet genannt wird. Die Karte kann zur Ausführung verschiedener Applets konfiguriert werden, die das Verhalten oder die Konfiguration der Smartcard ändern, ein Vorgang, der mit Personalisierung bezeichnet wird. Damit JavaCards mit PGP Desktop verwendet werden können, sind nur ein paar der verfügbaren Personalisierungsprofile anwendbar.

Zusätzlich müssen bei allen derzeit verfügbaren Personalisierungsprofilen geringfügige Änderungen an ihrer Konfiguration vorgenommen werden, damit sie mit PGP Desktop funktionieren. Insbesondere:

- Das Profil muss die PKCS-11-Unterstützung aktivieren. Meist erscheint der Name Netscape oder Entrust in den Titeln der Profile, die PKCS-11 unterstützen.
- Ein PGP Desktop-Schlüssel benutzt mindestens zwei private PKCS-11-Schlüssel. Damit ein Profil mit PGP Desktop verwendet werden kann, muss für die maximale Anzahl zulässiger privater Schlüssel der Wert 2 oder höher angegeben sein.

Weitere Informationen finden Sie in der Dokumentation der von Ihnen verwendeten JavaCard.

Kompatible Smartcards

Folgende Karten werden von PGP Desktop erkannt und unterstützt:

- DoD Common Access Cards (CACs) mit dem **ActivCard** Gold 2.0-Profil. Weitere Informationen zum ActivCard Gold 2.0-Profil finden Sie auf der *ActivCard-Website* (www.activcard.com).
- **AET SafeSign**-Smartcards, einschließlich ASEKey 1.0. Weitere Informationen zu Smartcards von AET SafeSign finden Sie auf der *Cryptoshop-Website* (www.cryptoshop.com).
- **Aladdin**-Smartcards, einschließlich eToken PRO USB 16K, 32K und 64K, Aladdin eToken NG-OTP 32K und eToken PRO Java. Weitere Informationen zu Aladdin eToken-Produkten finden Sie auf der *Support-Website von Aladdin* (http://www.aladdin.com/support/default.asp).

- **Athena Smartcard Solutions**-Smartcards, einschließlich des ASEKey USB-Tokens. Weitere Informationen zu Smartcards von Athena Smartcard Solutions finden Sie auf der *Athena Smartcard-Website* (www.athena-scs.com).
- **Axalto**-Smartcards (früher Schlumberger), einschließlich Cryptoflex 32K. Weitere Informationen zu Smartcards von Axalto finden Sie auf der *Axalto-Website* (www.axalto.com).
- **Axalto Cyberflex Access 32K V2**. Weitere Informationen zu Smartcards von Axalto finden Sie auf der *Axalto-Website* (www.axalto.com).
- **EMC RSA SecurID SID800-Token** (v1 and 2). Weitere Informationen zu Token von EMC finden Sie auf der *Website* (http://www.rsa.com/) von EMC/RSA.
- **Gemalto .NET v2**-Smartcards. Weitere Informationen zu Smartcards von Gemalto finden Sie auf der *Gemalto-Website* (http://www.gemalto.com).
- **GemPlus**-Smartcards, einschließlich SafesITe und GemXpresso Pro, unter Verwendung von GemSafe Libraries 4.2.0-015 (Gold). Weitere Informationen zu Smartcards von GemPlus finden Sie auf der *GemPlus-Website* (www.gemplus.com).
- **Giesecke and Devrient** Sm@rtCafe Expert 3.2-PIV-Karten, die die Clientsoftware ActivClient Version 6.1 verwenden. Weitere Informationen zu PIV-Karten von G&D finden Sie auf der *Website von Giesecke and Devrient* (http://www.gi-de.com/).
- **Oberthur** ID-One Cosmo V5.2D-PIV-Karten, die die Clientsoftware ActivClient Version 6.1 verwenden. Weitere Informationen zu PIV-Karten von Oberthur finden Sie auf der *Oberthur-Website* (http://www.oberthurcs.com/index.aspx).
- **SafeNet**-Smartcards, einschließlich iKey 2032. (PGP Desktop ist nicht mit SafeNet iKey 1000 oder 4000 kompatibel.) Weitere Informationen zu Smartcards und USB-Token von SafeNet finden Sie auf der *SafeNet-Website* (www.safenet-inc.com/products/tokens/index.asp).
- **T-Systems** Telesec NetKey 3.0- und TCOS 3.0 IEI-Karten. Weitere Informationen zu T-Telesec NetKey-Smartcards finden Sie auf der *T-Systems-Website* (www.t-systems.com).

PGP Desktop erkennt und unterstützt auch Smartcards anderer Anbieter, sofern in den entsprechenden Software-Treibern eine auf Standards basierte PKCS-11-Bibliothek enthalten ist. Falls eine nicht-standardmäßige Smartcard nicht mit PGP Desktop funktioniert, wird die Kennzeichnung **Smartcard-Schlüssel** nicht im Bedienfeld „PGP Keys“ angezeigt, wenn die Smartcard auf dem System installiert wird.

Smartcards erkennen

Bevor Sie die Eigenschaften einer Smartcard, die Sie mit PGP Desktop verwenden wollen, untersuchen können, oder vor dem Erstellen eines PGP-Schlüsselpaars auf einer Smartcard, müssen Sie sicherstellen, dass PGP Desktop bezeugt, dass die Smartcard, mit der Sie arbeiten möchten, auf dem System verfügbar ist.

Die allgemeinen Voraussetzungen dafür sind:

- Die Software-Treiber der Smartcard, die PKCS-11 unterstützen, müssen im System installiert sein.
- Die Smartcard muss auf dem System installiert sein. Bei USB-Tokens bedeutet dies im Allgemeinen, dass sie in einen USB-Port eingesteckt sind. Bei Smartcards bedeutet dies in der Regel, dass sie in das entsprechende Smartcard-Lesegerät eingelegt sind.

Sobald Sie Treiber und Smartcard installiert haben, überprüfen Sie, ob PGP Desktop das System erkennt. Hierzu gibt es zwei Möglichkeiten:

- Die einfachste Weise, um zu erfahren, ob PGP Desktop eine Smartcard „sieht", ist, PGP Desktop zu öffnen und auf das Bedienfeld „PGP Keys" zu klicken. Wenn im Bedienfeld „PGP Keys" unter „Alle Schlüssel" die Angabe „Smartcard-Schlüssel" erscheint, sieht PGP Desktop die Smartcard auf dem System.
- Ein etwas komplizierteres Verfahren besteht darin, PGP Desktop zu öffnen, auf das Bedienfeld „PGP Keys" zu klicken und dann vom Menü **Datei** die Option **Neuer PGP-Schlüssel** auszuwählen. Wenn der Bildschirm des Assistenten für die Erstellung eines PGP-Schlüssels angezeigt wird, sehen Sie sich die Informationen unten im Dialogfeld an. Wenn das Kontrollkästchen **Schlüssel auf Token erstellen: <Smartcard-Informationen>** aktiviert ist, erkennt PGP Desktop die Smartcard auf dem System. Diese Methode ist der vorausgehenden Methode dadurch überlegen, dass PGP Desktop Ihnen Informationen über die Smartcard anzeigt, die auf dem System erkannt wird.

Smartcard-Eigenschaften untersuchen

Ein auf einer Smartcard gespeicherter PGP-Schlüssel wird auf dem PGP Desktop-Bildschirm mit einem speziellen Symbol gekennzeichnet, einem Schlüssel auf einer Karte. In den Eigenschaften finden Sie Informationen zur Smartcard selbst, z. B. den Hersteller, die Seriennummer und die unterstützten Schlüsseltypen.

So zeigen Sie die Eigenschaften einer Smartcard an

1. Legen Sie die Smartcard in das Smartcard-Lesegerät ein oder stecken Sie das Token in einen USB-Anschluss. Der Schlüssel wird im Bedienfeld „PGP Keys“ im Abschnitt „Smartcard-Schlüssel“ angezeigt.
2. Öffnen Sie PGP Desktop.
3. Markieren Sie den Schlüssel, dessen Eigenschaften Sie sehen möchten.

   Wählen Sie **Schlüssel > Smartcard-Eigenschaften**. Das Dialogfeld „PGP Smartcard-Eigenschaften“ mit Informationen über die Smartcard, auf der sich der Schlüssel befindet, wird angezeigt:

   - Name des Herstellers
   - Smartcard-Modell
   - der Smartcard zugewiesene Seriennummer
   - Die Funktionen der Smartcard, einschließlich den Typ des PGP-Schlüssels, den die Karte speichern kann, und die Anzahl an Zeichen, die Ihre PIN enthalten kann
   - Die Gesamtanzahl der privaten Schlüssel, die sich derzeit auf der Smartcard befinden, einschließlich Unterschlüssel.
4. Klicken Sie auf **OK**.

Ein PGP-Schlüsselpaar auf einer Smartcard generieren

So generieren Sie ein PGP-Schlüsselpaar auf einer Smartcard

1. Legen Sie die Smartcard in das Smartcard-Lesegerät ein oder stecken Sie das Token in einen USB-Anschluss. Der Schlüssel wird im Bedienfeld „PGP Keys“ im Abschnitt „Smartcard-Schlüssel“ angezeigt.
2. Öffnen Sie PGP Desktop.
3. Klicken Sie auf das PGP-Schlüssel-Bedienfeld. Wird die Smartcard erkannt, wird im PGP Keys-Bedienfeld „Smartcard-Schlüssel“ angezeigt.
4. Gehen Sie auf **Datei > Neuer PGP-Schlüssel**. Das Dialogfeld „Einleitung zum PGP-Schlüsselerstellungs-Assistenten“ wird angezeigt.

   PGP Desktop erkennt die Software-Treiber jeweils eines Smartcard-Anbieters. Wenn auf Ihrem Computer Software-Treiber von mehr als einem Smartcard-Anbieter installiert sind, müssen Sie festlegen, von welchem Anbieter die Smartcard stammt, die Sie zusammen mit PGP Desktop verwenden möchten. Weitere Informationen finden Sie unter *Mehrere Smartcards verwenden* (auf Seite 321).

5 Aktivieren Sie das Kontrollkästchen **Schlüssel auf Token erstellen: [Name der Smartcard auf dem System]** und klicken Sie auf **Weiter**. Das Dialogfeld „Zuweisung von Name und E-Mail“ wird angezeigt.

6 Geben Sie im Feld **Vollständiger Name** Ihren Namen und im Feld **Primäre E-Mail** Ihre E-Mail-Adresse ein. Wenn Sie weitere E-Mail-Adressen für diesen Schlüssel eingeben möchten, klicken Sie auf **Mehr** und geben Sie die E-Mail-Adresse(n) in die Felder **Andere Adressen** ein.

Tipp: Es ist nicht zwingend erforderlich, Ihren tatsächlichen Namen oder Ihre E-Mail-Adresse einzugeben. Wenn Sie Ihren tatsächlichen Namen und Ihre richtige E-Mail-Adresse verwenden, können Sie von anderen Personen leichter als Eigentümer Ihres öffentlichen Schlüssels identifiziert werden.

7 Wenn Sie erweiterte Schlüsseleinstellungen festlegen möchten, klicken Sie auf **Erweitert**. Das Dialogfeld „Erweiterte Schlüsseleinstellungen“ wird angezeigt. Legen Sie die folgenden Einstellungen fest:

- **Schlüsseltyp:** RSA (Diffie-Hellman/DSS-Schlüssel werden nicht unterstützt)
- **Schlüsselgröße:** Von 1028 bis 2048
- **Ablaufdatum:** Nie oder ein von Ihnen festgelegtes Datum
- **Zulässige Algorithmen:** AES, CAST, TripleDes, IDEA und Twofish
- **Bevorzugter Algorithmus:** Wählen Sie einen der zulässigen Algorithmen aus
- **Zulässiger Hash-Algorithmus:** SHA-2-256, SHA-2-384, SHA-2-512, RIPEMD-160, SHA-1, MD-5
- **Bevorzugter Hash-Algorithmus:** Wählen Sie eine der zulässigen Hash-Funktionen aus

Bestimmte Einstellungen sind unter Umständen nicht verfügbar, wenn Sie von der von Ihnen verwendeten Smartcard nicht unterstützt werden.

Klicken Sie auf **OK**, um die Einstellungen zu speichern und das Dialogfeld „Erweiterte Schlüsseleinstellungen“ zu schließen.

8 Klicken Sie auf **Weiter**.

9 Geben Sie im Dialogfeld „Passphrasenzuweisung“ die PIN ein, die der Smartcard entspricht. Die PIN dient als Passphrase für den Schlüssel. Als zusätzliche Sicherheitsmaßnahme werden die für die Passphrase eingegebenen Zeichen in der Regel nicht auf dem Bildschirm angezeigt. Wenn Sie jedoch sicher sind, dass Sie nicht beobachtet werden, und die Zeichen beim Eingeben der Passphrase sehen möchten, aktiveren Sie das Kontrollkästchen **Tastatureingabe anzeigen.**

10 Klicken Sie auf **Weiter**, um mit der Schlüsselerstellung zu beginnen. Das neue Schlüsselpaar wird von PGP Desktop direkt auf der Smartcard erstellt. Dieser Vorgang kann einige Minuten dauern.

11 Wenn angezeigt wird, dass die Schlüsselerstellung abgeschlossen ist, klicken Sie auf **Weiter**. Sie werden aufgefordert, den öffentlichen Teil des soeben erstellten Schlüssels dem PGP Global Directory hinzuzufügen.

12 Lesen Sie den Text auf dem Bildschirm und führen Sie einen der folgenden Schritte aus:

- Wenn Sie Ihren öffentlichen Schlüssel in das PGP Global Directory einstellen möchten, klicken Sie auf **Weiter**.
- Wenn Sie nicht möchten, dass Ihr öffentlicher Schlüssel im PGP Global Directory eingestellt wird, klicken Sie auf **Überspringen**.

13 Klicken Sie auf **Fertig**. Das neue Schlüsselpaar wird erstellt und direkt auf Ihrer Smartcard gespeichert.

Da der private Teil Ihres Schlüsselpaars nur auf der Smartcard verbleibt, wenn Sie die Smartcard aus dem System entfernen, wechselt das Schlüsselsymbol zu einem einzelnen Schlüssel, um darzustellen, dass der öffentliche Teil auf dem Schlüsselbund verbleibt und der private Teil mit der Smartcard entfernt wurde.

Öffentliche Schlüssel von Smartcards auf Schlüsselbunde kopieren

Wenn Sie Ihre Schlüssel auf einer Smartcard speichern, können Sie zu einem Computer gehen (d. h. zu einem Computer mit kompatiblem Smartcard-Lesegerät oder einem freien USB-Anschluss, auf dem PGP Desktop sowie die entsprechenden Treiber installiert sind) und den *öffentlichen* Teil des Schlüsselpaars automatisch auf den PGP Desktop-Schlüsselbund auf diesem System kopieren.

So kopieren Sie den öffentlichen Schlüssel von der Smartcard auf den Schlüsselbund eines anderen Benutzers

1 Legen Sie die Smartcard in das Smartcard-Lesegerät ein oder stecken Sie das Token in einen USB-Anschluss. Der Schlüssel wird im Bedienfeld „PGP Keys“ im Abschnitt „Smartcard-Schlüssel“ angezeigt.

2 Öffnen Sie PGP Desktop.

3 Warten Sie, bis der Schlüssel in PGP Desktop angezeigt wird. Wenn der Schlüssel angezeigt wird, bedeutet dies, dass der öffentliche Schlüssel auf das System kopiert wurde.

4 Nehmen Sie die Smartcard aus dem System. Der öffentliche Schlüssel verbleibt auf dem System.

Schlüsselpaare vom Schlüsselbund auf eine Smartcard kopieren

Verwenden Sie PGP Desktop, um ein vorhandenes Schlüsselpaar vom System auf eine Smartcard zu kopieren. Diese Methode eignet sich besonders zum Sichern Ihres Schlüsselpaars und/oder Weitergeben des öffentlichen Schlüssels. Auf eine Smartcard können nur RSA-Schlüssel kopiert werden.

Hinweis: Diffie-Hellman/DSS-Schlüssel können nicht auf Smartcards kopiert werden.

Das Kopieren eines Schlüsselpaars auf eine Smartcard unterscheidet sich vom Erstellen eines Schlüsselpaars direkt auf der Smartcard (ein Vorgang, der nicht für alle Smartcards zur Verfügung steht). Wenn Sie ein Schlüsselpaar direkt auf einer Smartcard erstellen, *muss* sich die Smartcard auf dem System befinden, um den privaten Schlüssel verwenden zu können.

Wenn Sie ein vorhandenes Schlüsselpaar auf eine Smartcard kopieren, so befindet sich der private Abschnitt Ihres Schlüsselpaares sowohl auf der Smartcard, *als auch auf Ihrem System* (sofern Sie nicht den privaten Abschnitt Ihres Schlüsselpaares vom System löschen).

Es gibt zwei wichtige Gründe, ein vorhandenes Schlüsselpaar auf eine Smartcard zu kopieren:

- Wenn Sie die Kopie zur Datensicherung für das Schlüsselpaar auf dem System und zum Kopieren des öffentlichen Schlüssels von der Smartcard auf den Schlüsselbund anderer Personen verwenden möchten. In diesem Fall hätten Sie zwei Kopien desselben privaten Schlüssels: eine auf dem System, auf dem der Schlüssel ursprünglich erstellt wurde, und eine auf der Smartcard.
- Wenn Sie die Kopie als einzige Kopie des privaten Schlüssels verwenden möchten, als hätten Sie ihn direkt auf der Smartcard erstellt. In diesem Fall müssen Sie den privaten Schlüssel vom System löschen (eine entsprechende Option wird in PGP Desktop angezeigt). Wählen Sie diese Option aus, um den privaten Schlüssel vom System zu löschen, wenn Sie Smartcards erst verwenden, nachdem Sie bereits das PGP-Schlüsselpaar erstellt haben und die Vorteile nutzen möchten, die ein auf der Smartcard gespeichertes Schlüsselpaar bietet, jedoch kein neues Schlüsselpaar erstellen möchten.

Wenn Sie das PGP-Schlüsselpaar auf eine Smartcard kopieren, wird die Passphrase für das Schlüsselpaar auf der Smartcard automatisch zur PIN der Smartcard geändert. Die Passphrase für das Schlüsselpaar, das sich bereits auf dem System befand, d. h. das Schlüsselpaar, das Sie auf die Smartcard kopiert haben, *wird jedoch nicht geändert*. Sie haben zwei Kopien des gleichen Schlüsselpaar, jede mit eigener Passphrase.

Wenn Sie den privaten Schlüssel vom System löschen und ihn nur auf der Smartcard behalten möchten, verwenden Sie einfach die PIN der Smartcard als Passphrase für den privaten Schlüssel.

So kopieren Sie ein vorhandenes PGP-Schlüsselpaar auf die Smartcard

1. Legen Sie die Smartcard in das Smartcard-Lesegerät ein oder stecken Sie das Token in einen USB-Anschluss. Der Schlüssel wird im Bedienfeld „PGP Keys“ im Abschnitt „Smartcard-Schlüssel“ angezeigt.
2. Öffnen Sie PGP Desktop.
3. Klicken Sie mit der rechten Maustaste auf das Schlüsselpaar, das Sie kopieren möchten, und wählen Sie **Hinzufügen > Smartcard-Schlüssel** aus. Sie werden in einer Warnung darüber informiert, dass die PGP-Passphrase für dieses Schlüsselpaar nach dem Kopieren auf die Smartcard automatisch zur Smartcard-PIN geändert wird.
4. Klicken Sie auf **OK**, um fortzufahren. Das Dialogfeld „PGP-Passphrase eingeben“ wird angezeigt.
5. Geben Sie die Passphrase des Schlüssels ein und klicken Sie auf **OK**. Das Dialogfeld „PGP-Passphrase eingeben“ wird angezeigt.
6. Geben Sie die Smartcard-PIN ein und klicken Sie auf **OK**. Das Schlüsselpaar wird auf die Smartcard kopiert. Sie werden in PGP Desktop gefragt, ob Sie den privaten Teil des Schlüsselpaars vom Schlüsselbund entfernen möchten, sodass er sich nur noch auf der Smartcard befindet.
7. Führen Sie einen der folgenden Schritte aus:
   - Wenn Sie den privaten Teil des Schlüsselpaars vom Schlüsselbund entfernen möchten, klicken Sie auf **Ja**. Der private Teil des Schlüsselpaars wird vom Schlüsselbund auf dem System gelöscht und ist nur noch auf der Smartcard vorhanden.
   - Wenn Sie den privaten Teil des Schlüsselpaars auf dem Schlüsselbund beibehalten möchten, klicken Sie auf **Nein**. Der private Teil wird nicht gelöscht. Sie verfügen jetzt über zwei Kopien desselben Schlüsselpaars: eine auf dem System und die andere auf der Smartcard oder dem Token.

Schlüssel von der Smartcard sicher löschen

Sie können alle auf einer Smartcard gespeicherten Daten löschen, indem Sie im Dialogfeld für die Smartcard-Eigenschaften die Funktion **Inhalte sicher löschen** verwenden.

So löschen Sie den Inhalt einer Smartcard sicher

1. Legen Sie die Smartcard in das Smartcard-Lesegerät ein oder stecken Sie das Token in einen USB-Anschluss. Der Schlüssel wird im Bedienfeld „PGP Keys“ im Abschnitt „Smartcard-Schlüssel“ angezeigt.
2. Öffnen Sie PGP Desktop.
3. Wählen Sie in PGP Keys die Option **Smartcard-Schlüssel** aus. Die PGP-Schlüssel auf der Smartcard werden angezeigt.
4. Wählen Sie die Smartcard oder Token aus, die Sie sicher löschen möchten.
5. Klicken Sie auf **Schlüssel > Smartcard sicher löschen**. Sie müssen in PGP Desktop bestätigen, dass Sie alle derzeit auf der Smartcard bzw. auf dem Token gespeicherten Schlüssel löschen möchten.
6. Klicken Sie auf **OK**. Das Dialogfeld „PGP-Passphrase eingeben“ wird angezeigt.
7. Geben Sie die PIN für diese Smartcard ein. Als zusätzliche Sicherheitsmaßnahme werden die für die Passphrase eingegebenen Zeichen in der Regel nicht auf dem Bildschirm angezeigt. Wenn Sie jedoch sicher sind, dass Sie nicht beobachtet werden, und die Zeichen beim Eingeben der Passphrase sehen möchten, aktivieren Sie das Kontrollkästchen **Tastatureingabe anzeigen**.
8. Klicken Sie auf **OK**. Alle auf der Smartcard gespeicherten Schlüssel werden von PGP Desktop gelöscht.

Mehrere Smartcards verwenden

PGP Desktop ist mit Smartcards von einer Vielzahl von Anbietern kompatibel. PGP Desktop kann jedoch nur mit den Smartcards eines einzigen Anbieters gleichzeitig arbeiten.

Beim Starten sucht PGP Desktop automatisch in Ihrem System nach Software-Treibern, die die Verwendung der Smartcards eines bestimmten Anbieters unterstützen. Wenn die Anwendung die betreffenden Software-Treiber findet, werden diese geladen in der Annahme, dass Sie Smartcards von diesem Anbieter besitzen und diese benutzen wollen.

Falls auf Ihrem System die Software-Treiber eines einzelnen Anbieters installiert sind, läuft dies perfekt ab; PGP Desktop findet automatisch die Software-Treiber und ermöglicht die Verwendung der Smartcards dieses Anbieters. Sie brauchen nichts zu tun, es funktioniert einfach.

Es kann jedoch auch Fälle geben, in denen Sie Smartcards von mehr als einem Anbieter verwenden müssen. In solchen Fällen, und wenn auf einem System die Software-Treiber von mehr als einem Anbieter vorhanden sind, müssen Sie PGP Desktop angeben, wessen Smartcards Sie benutzen wollen. Andernfalls weiß PGP Desktop nicht, welche Software-Treiber zu verwenden sind, und wählt möglicherweise nicht diejenigen aus, die Sie wünschen.

So geben Sie an, welcher Smartcard-Software-Treiber verwendet werden soll

1. Öffnen Sie PGP Desktop.
2. Klicken Sie auf **Extras > PGP-Optionen**. Das Dialogfeld „PGP-Optionen“ wird angezeigt.
3. Klicken Sie auf die Registerkarte „Schlüssel“.
4. Wählen Sie im Abschnitt **Synchronisierung** aus der Liste **Schlüsselbund mit Token und Smartcards synchronisieren** **den Anbieter des zu verwendenden Software-Treibers aus:**
   - Wenn auf dem System nur Software-Treiber eines Anbieters installiert sind, verwenden Sie die Standardeinstellung **Automatisch**.
   - Wählen Sie **Keine** aus, um zu verhindern, dass PGP Desktop Smartcards von anderen Anbietern verwendet.
   - Wenn Sie einen Anbieter angeben möchten, der *nicht* in der Liste aufgeführt ist, wählen Sie **Andere** aus.Wechseln Sie im Dialogfeld „Smartcard-Treiber auswählen“ zur DLL-Datei der Software-Treiber Ihres Smartcard-Anbieters, wählen Sie die Datei aus und klicken Sie auf **Öffnen**.Jetzt können Sie Smartcards verwenden, die von dem von Ihnen ausgewählten Software-Treiber unterstützt werden.

PGP Desktop erwartet nun, dass Sie Smartcards des ausgewählten Anbieters verwenden. Wenn Sie eine Smartcard eines anderen Anbieters zu Ihrem System hinzufügen, wird diese von PGP Desktop nicht erkannt. Sie müssen dieses Verfahren wiederholen, um auf einen anderen Smartcard-Anbieter zu wechseln.

Sonder-Token

PGP Desktop verwendet das USB-Token Aladdin eToken Pro zur Authentifizierung beim Systemstart, wenn das *Startlaufwerk* vollständig verschlüsselt wurde (weitere Informationen zum Schützen eines Startlaufwerks mit PGP Whole Disk Encryption finden Sie unter *Laufwerke mit PGP Whole Disk Encryption schützen* (auf Seite 155)). Nur das USB-Token Aladdin eToken Pro kann zu diesem Zweck verwendet werden. Weitere Informationen zum Konfigurieren dieses Tokens finden Sie unter *Aladdin eToken konfigurieren* (auf Seite 323).

Aladdin eToken konfigurieren

Sie benötigen ein USB-Token Aladdin eToken Pro mit einem PGP-Schlüsselpaar zur Verwendung mit der PGP Whole Disk Encryption-Funktion von PGP Desktop für Windows.

So erstellen Sie ein USB-Token Aladdin eToken Pro zur Verwendung mit PGP Whole Disk Encryption

1. Erwerben Sie ein USB-Token Aladdin eToken Pro. Dies ist das einzige Token, das mit PGP Whole Disk Encryption verwendet werden kann. Verwenden Sie eines der drei Modelle: 16K, 32K oder 64K. Die 16K- und 32K-Modelle unterstützen Schlüssel von 1024 Bit, das 64K-Modell unterstützt Schlüssel bis 2048 Bit.
2. Stellen Sie sicher, dass die entsprechende Treibersoftware von Aladdin auf dem System installiert ist. Weitere Informationen zu den Aladdin-Treibern finden Sie unter *Erforderliche Treiber für das Aladdin eToken* (auf Seite 175).

   Wenn die Treibersoftware installiert ist, zeigt PGP Desktop im Bedienfeld „PGP-Schlüssel“ die Option **Smartcard-Schlüssel** an.
3. Öffnen Sie PGP Desktop für Windows.
4. Erstellen Sie ein Schlüsselpaar auf dem Aladdin eToken (Anleitungen hierzu finden Sie unter *PGP-Schlüsselpaare auf Smartcards erstellen* (siehe "Ein PGP-Schlüsselpaar auf einer Smartcard generieren" auf Seite 316)) oder verwenden Sie im Kontextmenü die Option **Hinzufügen zu**, um ein bestehendes Schlüsselpaar auf das Token zu kopieren (Anleitungen hierzu finden Sie unter *Öffentliche Schlüssel von Smartcards auf Schlüsselbunde kopieren* (siehe "Schlüsselpaare vom Schlüsselbund auf eine Smartcard kopieren" auf Seite 319)).

   Wenn Sie ein bestehendes Schlüsselpaar an das Token senden möchten, muss es sich um einen RSA-Schlüssel mit 1024 Bit oder 2048 Bit handeln. Das Aladdin eToken Pro unterstützt derzeit keine anderen Schlüsselgrößen oder DH/DSS-Schlüssel.

   Wenn Sie ein Schlüsselpaar auf dem Token erstellen oder ein bestehendes Schlüsselpaar an das Token senden, ändert sich die Passphrase des Schlüsselpaars zur PIN des Tokens. Die Standard-PIN für das Aladdin eToken Pro ist 1234567890. Da diese Standard-PIN allgemein bekannt ist, sollten Sie sie unbedingt mit der Aladdin-Software ändern.
5. Sie können jetzt das PGP-Schlüsselpaar auf dem Aladdin eToken mit PGP Whole Disk Encryption verwenden.

A PGP Desktop-Optionen festlegen

*Die in diesem Abschnitt beschriebenen Leistungsmerkmale finden nur dann Anwendung, wenn Sie PGP Desktop Virtual Disk Professional installiert haben. Welche Version Sie verwenden, können Sie aus dem Abschnitt unter Lizenzierung entnehmen.*PGP Desktop wurde auf die Anforderungen der meisten Benutzer zugeschnitten, jedoch können Sie einige Einstellungen Ihren spezifischen Anforderungen entsprechend anpassen. In diesem Abschnitt werden die Optionen und ihre Einstellungsmöglichkeiten in PGP Desktop erläutert.

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung verwenden, hat Ihr PGP Universal Server-Administrator ggf. bestimmte Funktionen deaktiviert. Ist eine Funktion deaktiviert, wird das Bedienelement auf der linken Seite nicht angezeigt und das Menü oder andere auf diese Funktion zutreffenden Optionen sind nicht verfügbar. Die in diesem Handbuch enthaltenen Abbildungen entsprechen der Standardinstallation, bei der alle Funktionen aktiviert sind. Wenn Ihr PGP Universal Server-Administrator diese Funktion deaktiviert hat, ist dieser Abschnitt für Sie nicht relevant.

In diesem Kapitel

Zugriff auf das Dialogfeld PGP-Optionen 326
Allgemeine Optionen 327
Schlüsseloptionen 330
Hauptschlüsseloptionen 333
Messaging-Optionen 334
PGP NetShare-Optionen 340
Laufwerksoptionen 342
Notifier-Optionen 345
Erweiterte Optionen 347

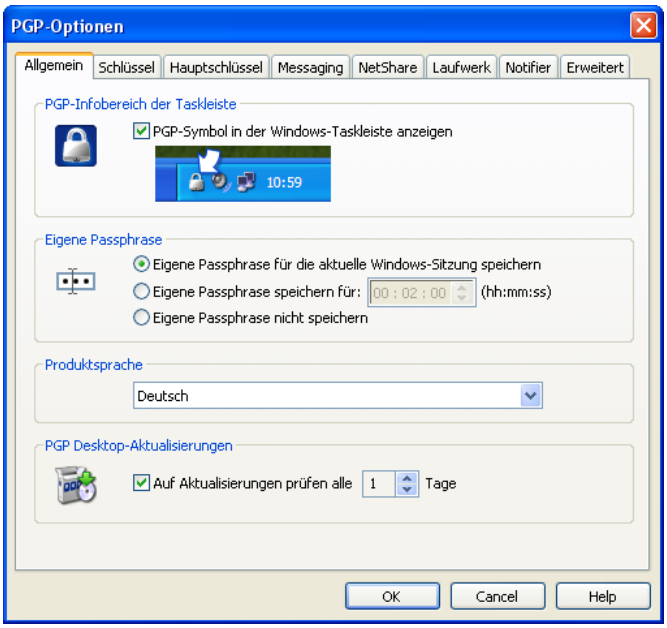
Zugriff auf das Dialogfeld PGP-Optionen

Die in diesem Abschnitt beschriebenen Leistungsmerkmale finden nur dann Anwendung, wenn Sie PGP Desktop Virtual Disk Professional installiert haben. Welche Version Sie verwenden, können Sie aus dem Abschnitt unter Lizenzierung entnehmen.**So greifen Sie auf die PGP-Optionen zu**

1. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf das PGP-Symbol **im Infobereich der Windows-Taskleiste und wählen Sie Optionen** aus.
   - Öffnen Sie PGP Desktop und wählen Sie **Extras > PGP Optionen** aus.
2. Wählen Sie eine Registerkarte aus und nehmen Sie die gewünschten Änderungen vor. Wenn Sie mit einer bestimmten Registerkarte fertig sind, wählen Sie eine andere Registerkarte aus.
3. Wenn Sie die Änderungen speichern und den Vorgang beenden möchten, klicken Sie auf **OK**. Wenn Sie die vorgenommenen Änderungen nicht übernehmen möchten, klicken Sie auf **Abbrechen**.

Allgemeine Optionen

*Die in diesem Abschnitt beschriebenen Leistungsmerkmale finden nur dann Anwendung, wenn Sie PGP Desktop Virtual Disk Professional installiert haben. Welche Version Sie verwenden, können Sie aus dem Abschnitt unter Lizenzierung entnehmen.*Die Registerkarte „Allgemein“ umfasst verschiedene PGP Desktop-Einstellungen.



Die Registerkarte „Allgemein“ im Dialogfeld „Einstellungen“ enthält folgende Optionen:

- **PGP-Symbol in der Windows-Taskleiste anzeigen**: Wenn diese Option aktiviert ist, wird das PGP-Symbol in der Windows-Taskleiste angezeigt, während PGP Desktop auf dem System aktiv ist. Über das PGP-Symbol im Infobereich der Taskleiste können Sie problemlos auf Funktionen von PGP Desktop zugreifen. Deaktivieren Sie das Kontrollkästchen, um das PGP-Symbol aus der Windows-Taskleiste zu entfernen. Stellen Sie das PGP-Symbol wieder her, indem Sie PGP Desktop starten und im Menü **Extras** die Option **PGP-Optionen** auswählen. **Öffnen Sie die Registerkarte „Allgemein“ und aktivieren Sie das Kontrollkästchen.**

  Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, ist diese Option möglicherweise erforderlich.

  Durch Entfernen des PGP-Symbols aus der Windows-Taskleiste werden die PGP Desktop-Dienste nicht heruntergefahren. PGP Desktop-Dienste werden weiterhin ausgeführt, auch wenn das PGP-Symbol aus der Windows-Taskleiste entfernt wurde.

Wenn Sie die PGP-Dienste anhalten möchten, klicken Sie auf das PGP-Symbol im Infobereich der Taskleiste. Wählen Sie aus der Liste der angezeigten Befehle die Option **PGP-Dienste beenden** aus. In einem Warndialogfeld werden Sie aufgefordert, den Vorgang zu bestätigen.

Hinweis: Die PGP Corporation empfiehlt, die PGP Desktop-Dienste nur bei Bedarf anzuhalten.

- **Eigene Passphrase**: Bietet Optionen zum Speichern der Passphrase.
  - **Eigene Passphrase für die aktuelle Windows-Sitzung speichern**: Speichert die Passphrase automatisch, bis Sie sich vom Computer abmelden. Dieser Vorgang wird als *Zwischenspeicherung* der Passphrase bezeichnet. Wenn diese Option aktiviert ist, werden Sie für jeden privaten Schlüssel einmal zur Eingabe der Passphrase aufgefordert. Sie müssen die Passphrase bis zum Abmelden vom Computer nicht erneut für den Schlüssel eingeben

Achtung: Wenn diese Option aktiviert ist, ist es äußerst wichtig, dass Sie sich vom Computer abmelden, bevor Sie ihn verlassen. Falls Sie sich nie abmelden, kann die Passphrase wochenlang zwischengespeichert bleiben. Unbefugte Personen können in diesem Fall Ihre verschlüsselten Nachrichten lesen oder Nachrichten mit Ihrem Schlüssel verschlüsseln, wenn Sie sich nicht am Computer befinden. Wenn Sie in der Regel für längere Zeit am Computer angemeldet sind, wählen Sie eine der anderen Zwischenspeicherungsoptionen.

  - **Eigene Passphrase für X (hh:mm:ss) speichern**: Speichert die Passphrase für den angegebenen Zeitraum automatisch im Speicher. Wenn Sie diese Option aktivieren, werden Sie einmal für die erste Signierungs- oder Entschlüsselungsaufgabe zur Eingabe der Passphrase aufgefordert. Sie werden während des festgelegten Zeitraums nicht erneut zur Eingabe der Passphrase aufgefordert. Die Standardeinstellung ist 00:02:00 (2 Minuten).
  - **Eigene Passphrase nicht speichern**: Verhindert, dass die Passphrase im Speicher abgelegt wird. Wenn Sie diese Option aktivieren, müssen Sie die Passphrase immer eingeben, wenn sie benötigt wird.

    Auch wenn Sie sich entscheiden, die Passphrase nicht zu speichern, werden Sie nur einmal zur Eingabe der Passphrase aufgefordert, wenn Sie auf alle Dateien in einem Ordner zugreifen möchten, der zu PGP NetShare hinzugefügt wurde.
- **Produktsprache**: Wählen Sie die Sprache für die Benutzeroberfläche von PGP Desktop aus. Folgende Optionen sind verfügbar: Englisch (Standard), Deutsch, Französisch, Japanisch und Spanisch.

Hinweis: Sie müssen sich beim System ab- und wieder anmelden, wenn Sie zu einer anderen Sprache wechseln möchten.

- **Alle X Tage auf Aktualisierungen prüfen:** Wenn diese Option aktiviert ist, prüft PGP Desktop in festgelegten Intervallen automatisch, ob Softwareaktualisierungen verfügbar sind. Das Standardintervall beträgt einen Tag. Wenn eine neuere Version von PGP Desktop zum Herunterladen verfügbar ist, wird ein Benachrichtigungsbildschirm angezeigt, über den Sie die neue Version herunterladen können. Ist diese Option deaktiviert, prüft PGP Desktop nicht automatisch, ob Softwareaktualisierungen verfügbar sind.

  Für diese Option ist eine aktive Internetverbindung erforderlich.

  Laden Sie die Aktualisierung herunter und installieren Sie sie, indem Sie den Aufforderungen folgen.

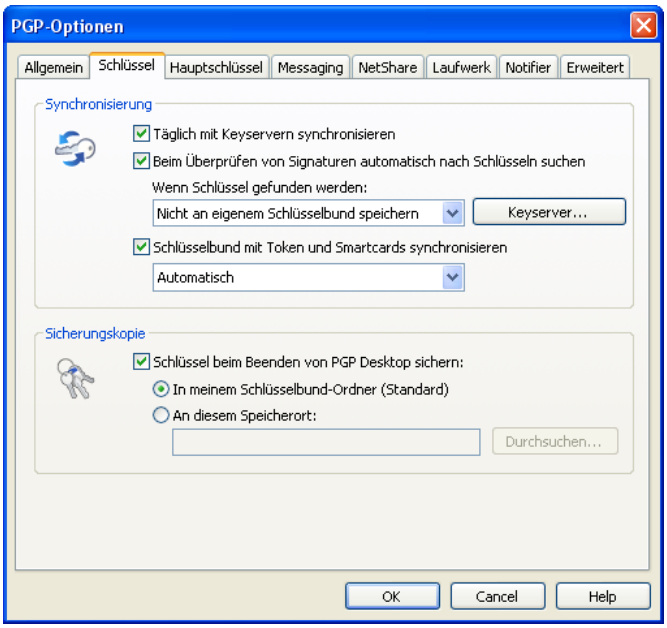
  Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung verwenden, ist diese Option möglicherweise erforderlich. PGP Desktop sucht dann auf dem entsprechend zugeordneten PGP Universal Server nach Aktualisierungen.

  Hinweis: Sie müssen auf dem System über Administratorrechte verfügen, um die Aktualisierung installieren zu können.

  Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung verwenden, ist diese Option möglicherweise erforderlich. PGP Desktop sucht dann auf dem entsprechend zugeordneten PGP Universal Server nach Aktualisierungen.

Schlüsseloptionen

*Die in diesem Abschnitt beschriebenen Leistungsmerkmale finden nur dann Anwendung, wenn Sie PGP Desktop Virtual Disk Professional installiert haben. Welche Version Sie verwenden, können Sie aus dem Abschnitt unter Lizenzierung entnehmen.*Die Registerkarte „Schlüssel“ enthält Einstellungen für PGP Desktop-Schlüssel.



Auf der Registerkarte „Schlüssel“ sind folgende Optionen verfügbar:

- **Synchronisierung**: Mit diesen Einstellungen wird festgelegt, wie Schlüssel auf Schlüsselbunden mit den öffentlichen Servern synchronisiert werden.
  - **Täglich mit Keyservern synchronisieren**: Wenn diese Option ausgewählt ist, führt PGP Desktop täglich eine Synchronisierung der öffentlichen Schlüssel am Schlüsselbund mit der Liste der Keyserver durch. Diese Liste enthält auch das PGP Global Directory.

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, ist diese Option möglicherweise erforderlich.

Sind geänderte Versionen der Schlüssel verfügbar, werden sie automatisch heruntergeladen. Wenn PGP Desktop vom Keyserver benachrichtigt wird, dass ein Schlüssel vom Keyserver entfernt wurde, deaktiviert PGP Desktop diesen Schlüssel am lokalen Schlüsselbund.

Wenn Sie mit PGP Desktop eine Änderung an einem Schlüsselpaar am Schlüsselbund vornehmen, wird diese Änderung nicht automatisch vom Computer auf den Keyserver hochgeladen. Sie müssen den geänderten Schlüssel manuell auf den gewünschten Keyserver hochladen. Wenn Sie PGP Desktop beenden, werden Sie von PGP Desktop zum Hochladen geänderter Schüssel aufgefordert. Sie können den Schlüssel jedoch auch an den Keyserver senden, indem Sie mit der rechten Maustaste auf den geänderten Schlüssel klicken, aus dem Kontextmenü die Option zum Senden auswählen **und dann in der Liste auf den gewünschten Keyserver klicken.**

- **Beim Überprüfen von Signaturen automatisch nach Schlüsseln suchen**: Wenn diese Option aktiviert ist, können Sie festlegen, dass PGP Desktop die konfigurierten Keyserver nach einem verifizierten Schlüssel durchsucht, wenn die öffentlichen Schlüssel am lokalen Schlüsselbund nicht vorhanden sind.

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, wird diese Option nicht verwendet. Der PGP Universal Server definiert, ob Schlüssel gesucht und, wenn gefunden, zwischengespeichert werden. Schlüssel, die in einer von einem PGP Universal Server verwalteten Umgebung gefunden werden, werden nie am Schlüsselbund gespeichert.

Wenn der öffentliche Schlüssel gefunden wird, stehen drei Optionen zur Auswahl:

- **Nicht an eigenem Schlüsselbund speichern**: Alle auf den konfigurierten Keyservern gefundenen Schlüssel werden nur einmal verwendet, um die Signatur zu verifizieren, mit der Sie gegenwärtig arbeiten Der Schlüssel wird anschließend nicht am Schlüsselbund gespeichert.
- **Zum Speichern an eigenem Schlüsselbund auffordern**: Legt fest, dass PGP Desktop eine Aufforderung anzeigt, um das Speichern der gefundenen Schlüssel am lokalen Schlüsselbund von Ihnen bestätigen zu lassen.
- **Schlüssel an eigenem Schlüsselbund speichern:** Legt fest, dass gefundene Schlüssel automatisch am lokalen Schlüsselbund gespeichert werden.

- **Schlüsselbund mit Token und Smartcards synchronisieren**: Legen Sie fest, wie PGP Desktop die Synchronisierung mit Smartcards und Token durchführt:
  - **Automatisch**: PGP Desktop lädt und verwendet automatisch den PKCS-11-Treiber des ersten Smartcard- bzw. Token-Anbieters, der auf dem System gefunden wird. Wählen Sie diese Einstellung aus, wenn auf dem System der PKCS-11-Treiber nur eines Smartcard- bzw. Token-Anbieters installiert ist. PGP Desktop erkennt und verwendet dann automatisch die Smartcards bzw. Token dieses Anbieters.

- **Aufgelisteter Anbieter**: PGP Desktop lädt und verwendet den PKCS-11-Treiber des Smartcard- bzw. Token-Anbieters, den Sie in der Liste auswählen. Wenn auf dem System die PKCS-11-Treiber mehrerer Smartcard- bzw. Token-Anbieter installiert sind, legen Sie in PGP Desktop mit dieser Einstellung den Anbieter fest, dessen Smartcards bzw. Token verwendet werden sollen.
- **Andere**: Ermöglicht die Auswahl eines PKCS-11-Treibers über das angezeigte Dialogfeld **Smartcard-Treiber auswählen**. Wenn Sie diese Option auswählen, erkennt und verwendet PGP Desktop die Smartcards bzw. Token des Anbieters, dessen PKCS-11-Treiber Sie auswählen. Verwenden Sie diese Einstellung, wenn Sie Smartcards bzw. Token von Anbietern verwenden möchten, die nicht aufgeführt sind.

Wenn die PKCS-11-Bibliothek eines Smartcard-Anbieters auf dem System installiert ist und mit anderen PKCS-11-Anwendungen (z. B. Mozilla Firefox oder Thunderbird) funktioniert, ist die Wahrscheinlichkeit groß, dass PGP Desktop Smartcards von diesem Anbieter erkennen und verwenden kann.

Falls eine nicht-standardmäßige Smartcard nicht mit PGP Desktop funktioniert, wird die Kennzeichnung „Smartcard-Schlüssel“ *nicht* im Bedienfeld „PGP Keys“ angezeigt, wenn die Smartcard auf dem System installiert wird.

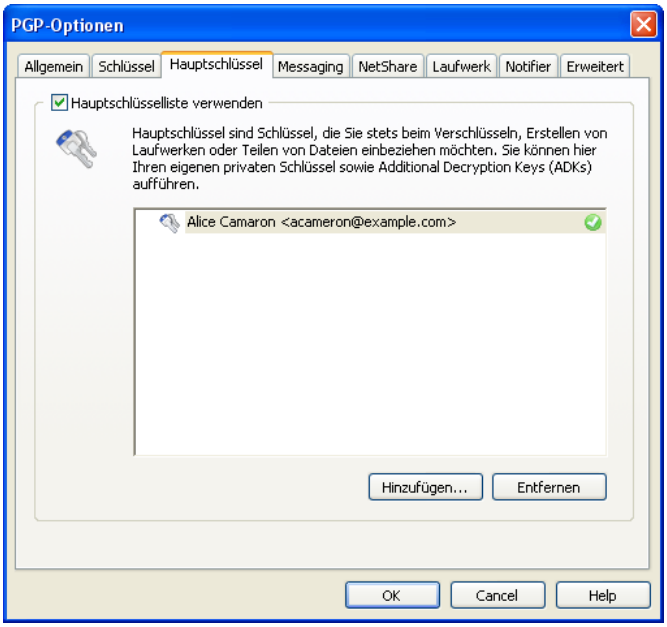
- **Keine**: PGP Desktop erkennt und unterstützt keine Smartcards oder Token auf dem System.

- **Keyserver**: Klicken Sie, um das Dialogfeld „PGP-Keyserver-Liste“ anzuzeigen. Verwenden Sie dieses Dialogfeld, um in der Liste Keyserver, die bei der automatischen Schlüsselsuche verwendet werden sollen, hinzuzufügen, zu bearbeiten oder zu entfernen.

- **Sicherungskopie**: Mit diesen Einstellungen wird festgelegt, wann und wo die Schlüssel gesichert werden sollen.
  - **Schlüssel beim Beenden von PGP sichern:** Wenn diese Option aktiviert ist, sichert PGP Desktop die Schlüssel automatisch am angegebenen Speicherort:
    - **In eigenem Schlüsselbund-Ordner (Standard):** Wenn diese Option ausgewählt ist, werden die Schlüssel im standardmäßigen Schlüsselbund-Ordner auf dem System gesichert. Der Standardspeicherort ist der Ordner „Eigene Dateien“.
    - **An diesem Speicherort:** Wenn diese Option ausgewählt ist, werden die Schlüssel an einem von Ihnen festgelegten Speicherort auf dem Computer gesichert. Geben Sie den vollständigen Dateipfad ein oder klicken Sie auf **Durchsuchen**, um zu einem Speicherort zu wechseln.

Hauptschlüsseloptionen

*Die in diesem Abschnitt beschriebenen Leistungsmerkmale finden nur dann Anwendung, wenn Sie PGP Desktop Virtual Disk Professional installiert haben. Welche Version Sie verwenden, können Sie aus dem Abschnitt unter Lizenzierung entnehmen.*Die Hauptschlüsselliste enthält eine Reihe von Schlüsseln, die Sie standardmäßig jedes Mal hinzufügen möchten, wenn Sie Schlüssel für Messaging, Laufwerksverschlüsselung, PGP NetShare oder PGP Zip auswählen. Die betreffenden Schlüssel müssen in diesem Fall nicht mehr in das Feld **Empfänger** gezogen werden.



Wenn Sie die Hauptschlüsselliste verwenden möchten, aktivieren Sie das Kontrollkästchen **Hauptschlüssellisteverwenden. Sie können nur Schlüssel in die Hauptschlüsselliste aufnehmen bzw. daraus entfernen, wenn dieses Kontrollkästchen aktiviert ist.**

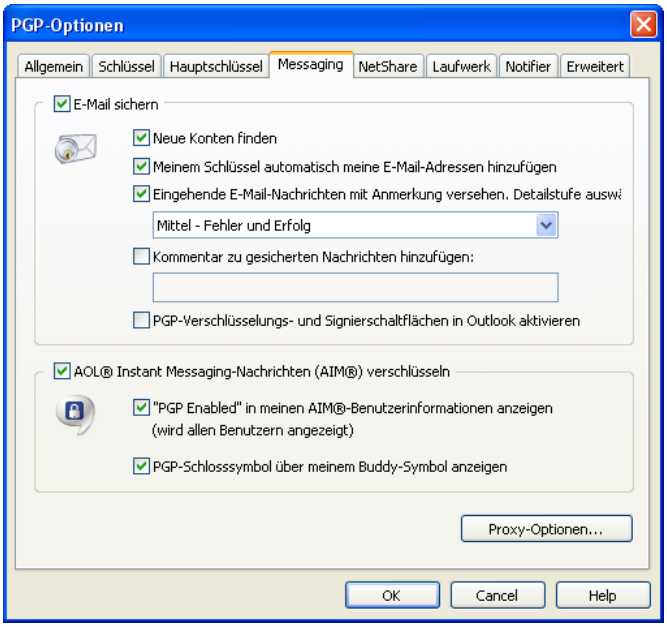
Weitere Informationen zum Hinzufügen von Hauptschlüsseln finden Sie unter *Der Hauptschlüsselliste Schlüssel hinzufügen* (auf Seite 58). Weitere Informationen zum Löschen von Hauptschlüsseln finden Sie unter *Schlüssel aus der Hauptschlüsselliste löschen* (auf Seite 59).

Hinweis: Wenn Sie Ihren Schlüssel mithilfe des Einrichtungsassistenten erstellt haben, wird er der Hauptschlüsselliste automatisch hinzugefügt. Wenn Sie die Schlüsselerstellung übersprungen und den Schlüssel in PGP Desktop importiert haben, wird der Schlüssel nicht automatisch der Liste hinzugefügt.

Messaging-Optionen

*Die in diesem Abschnitt beschriebenen Leistungsmerkmale finden nur dann Anwendung, wenn Sie PGP Desktop Virtual Disk Professional installiert haben. Welche Version Sie verwenden, können Sie aus dem Abschnitt unter Lizenzierung entnehmen.*Die Registerkarte „Messaging“ enthält Einstellungen für E-Mail-Nachrichten und Instant Messaging.

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung verwenden, hat Ihr PGP Universal Server-Administrator ggf. bestimmte Funktionen deaktiviert. Ist eine Funktion deaktiviert, wird das Bedienelement auf der linken Seite nicht angezeigt und das Menü oder andere auf diese Funktion zutreffenden Optionen sind nicht verfügbar. Die in diesem Handbuch enthaltenen Abbildungen entsprechen der Standardinstallation, bei der alle Funktionen aktiviert sind. Wenn Ihr PGP Universal Server-Administrator diese Funktion deaktiviert hat, ist dieser Abschnitt für Sie nicht relevant.



Auf der Registerkarte „Messaging“ sind folgende Optionen verfügbar:

- **E-Mail sichern:** Aktivieren Sie das Kontrollkästchen **E-Mail sichern**, wenn Ihre gesamten E-Mail-Konten automatisch von PGP Desktop gesichert werden sollen. Wenn diese Option aktiviert ist, fängt PGP Desktop alle eingehenden und ausgehenden E-Mail-Nachrichten ab und sichert sie entsprechend der jeweiligen Richtlinien.

  Deaktivieren Sie das Kontrollkästchen **E-Mail sichern**, wenn Ihre E-Mail-Konten nicht mehr von PGP Desktop gesichert werden sollen.

Wenn Sie das Kontrollkästchen **E-Mail sichern** aktivieren, können Sie zusätzlich folgende Optionen auswählen:

- **Neue Konten finden:** Aktivieren Sie dieses Kontrollkästchen, wenn PGP Desktop Ihre E-Mail-Aktivitäten überwachen und automatisch nach neuen, von Ihnen verwendeten E-Mail-Konten suchen soll. Wird ein neues Konto erkannt, werden Sie von PGP Desktop gefragt, ob über dieses Konto gesendete Nachrichten gesichert werden sollen.

Hinweis: Wenn Sie PGP Desktop in einer von PGP Universal verwalteten Umgebung einsetzen, unterbindet die Verwendung einer Platzhalterbindung (*) diese Funktion, da alle Maildienste der Platzhalterbindung * entsprechen. Daher entsprechen alle neuen Konten automatisch den Richtlinien und werden erstellt, auch wenn diese Option deaktiviert ist.

- **Meinem Schlüssel automatisch meine E-Mail-Adressen hinzufügen:**Wenn Sie dieses Kontrollkästchen aktivieren, fügt PGP Desktop Ihrem Schlüssel automatisch die zum Senden von Nachrichten verwendeten E-Mail-Adressen hinzu. Diese Option ist standardmäßig aktiviert. Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, ist diese Option möglicherweise deaktiviert.

  Deaktivieren Sie dieses Kontrollkästchen, damit E-Mail-Adressen dem Schlüssel nicht automatisch hinzugefügt werden. Dies dient dem Datenschutz. Sie können dadurch beispielsweise verhindern, dass jemand Ihre E-Mail-Adresse ermittelt.

- **Eingehende E-Mail-Nachrichten mit Anmerkung versehen:** Aktivieren Sie dieses Kontrollkästchen, wenn eingehende E-Mail-Nachrichten mit Anmerkungen versehen werden sollen, in denen die von PGP Desktop durchgeführten Verarbeitungsschritte beschrieben werden. Sie können zwischen drei Anmerkungsstufen wählen:
  - **Maximal: Ausführliche Anmerkung:** In den Anmerkungen wird jede Aktion beschrieben, die von PGP Desktop während der Verarbeitung durchgeführt wurde.
  - **Mittel: Fehler und Erfolg**: Dies ist die Standardoption. Es werden Anmerkungen hinzugefügt, wenn Verarbeitungsprobleme aufgetreten sind, z. B. unbekannte Schlüssel oder Signierer. Zudem werden bei dieser Einstellung Anmerkungen hinzugefügt, wenn die eingehende E-Mail-Nachricht erfolgreich entschlüsselt und/oder signiert wurde.
  - **Minimal: Nur Fehler:** Es werden nur Anmerkungen hinzugefügt, wenn bei der Verarbeitung Fehler aufgetreten sind.

- **Kommentar zu gesicherten Nachrichten hinzufügen:** Wenn diese Option aktiviert ist, wird der hier eingegebene Text stets in verschlüsselte oder signierte Nachrichten aufgenommen. In dieses Feld eingegebene Kommentare werden in jeder gesicherten Nachricht unterhalb der Textkopfzeile `--BEGIN PGP MESSAGE BLOCK--` und der Versionsnummer von PGP Desktop angezeigt. Diese Kommentare werden in entschlüsselten E-Mail-Nachrichten nicht angezeigt.
- **PGP-Verschlüsselungs- und Signierschaltflächen in Outlook aktivieren**: Aktivieren Sie dieses Kontrollkästchen, wenn Sie Verschlüsselungs- und Signierschaltflächen von PGP Desktop in Microsoft Outlook verwenden möchten. Diese Option ist standardmäßig deaktiviert. Weitere Informationen zu den Verschlüsselungs- und Signierschaltflächen finden Sie unter *Signier- und Verschlüsselungsschaltflächen in Microsoft Outlook verwenden* (auf Seite 100).

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, enthält dieses Feld möglicherweise bereits Text.

- **AOL® Instant Messaging-Nachrichten (AIM®) verschlüsseln:** Aktivieren Sie diese Option, wenn PGP Desktop Instant Messaging-Sitzungen mit kompatibler Instant Messaging-Software verschlüsseln soll.

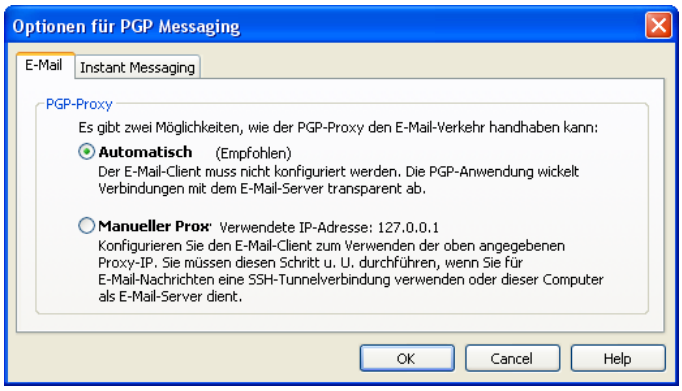
  Kompatibel sind AOL® Instant Messenger™ sowie kompatible Software.

  - **„PGP-aktiviert“ in meinen Benutzerinformationen (AIM) anzeigen**: Wenn diese Option aktiviert ist, wird der Hinweis **PGP-aktiviert** zusammen mit Ihrem Benutzernamen z. B. in der AIM-Buddy-Liste oder im Befehl zum Abrufen von Buddy-Informationen angezeigt. Ist die Option deaktiviert, wird Ihr Benutzername ohne den Hinweis **PGP-aktiviert** angezeigt.Das Erscheinungsbild dieses Textes kann abhängig vom jeweiligen Instant Messaging-Client variieren.
  - **PGP-Schlosssymbol über meinem Buddy-Symbol anzeigen**: Wenn diese Option aktiviert ist, wird das stilisierte PGP-Schlosssymbol über Ihrem Buddy-Symbol angezeigt. Andere Benutzer erkennen daran, dass die Instant Messaging-Sitzung geschützt ist. Ist die Option deaktiviert, wird Ihr Symbol normal angezeigt.

Proxy-Optionen

Klicken Sie auf die Schaltfläche **Proxy-Optionen**, um auf erweiterte Messaging-Optionen zuzugreifen.

Registerkarte „E-Mail“


Optionen für PGP Messaging
E-Mail
Instant Messaging
PGP-Proxy
Es gibt zwei Möglichkeiten, wie der PGP-Proxy den E-Mail-Verkehr handhaben kann:
Automatisch (Empfohlen)
Der E-Mail-Client muss nicht konfiguriert werden. Die PGP-Anwendung wickelt Verbindungen mit dem E-Mail-Server transparent ab.
Manueller Prox Verwendete IP-Adresse: 127.0.0.1
Konfigurieren Sie den E-Mail-Client zum Verwenden der oben angegebenen Proxy-IP. Sie müssen diesen Schritt u. U. durchführen, wenn Sie für E-Mail-Nachrichten eine SSH-Tunnelverbindung verwenden oder dieser Computer als E-Mail-Server dient.
OK
Cancel
Help

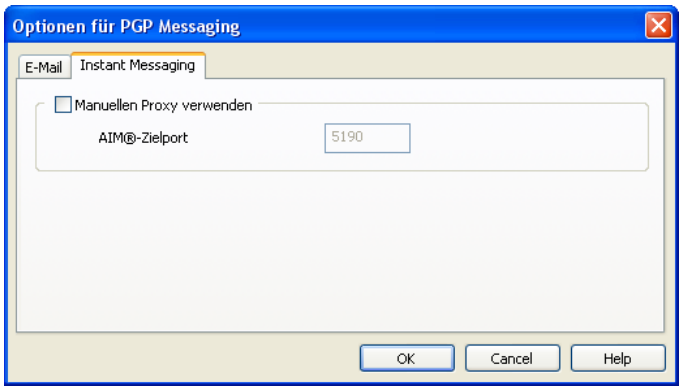
Verwenden Sie diese Registerkarte, wenn ein Proxy auf dem Computer manuell konfiguriert werden muss, damit Sie E-Mail-Nachrichten senden und empfangen können.

PGP Desktop ist zwischen Ihre E-Mail-Anwendung und den E-Mail-Server geschaltet, der für die Zustellung Ihrer E-Mail-Nachrichten zuständig ist. Dadurch kann PGP Desktop den Nachrichtenverkehr automatisch für Sie filtern bzw. als *Proxy* dienen. Auf diese Weise schützt PGP Desktop Ihre Nachrichten anhand der jeweiligen Richtlinie, ohne Sie bei der Arbeit zu behindern.

In der Regel müssen Sie die Proxyeinstellungen der PGP-Anwendung nicht ändern. In manchen Situationen müssen die Proxyeinstellungen jedoch manuell festgelegt werden. Verwenden Sie die vom Netzwerkadministrator empfohlene Einstellung:

- **Automatisch:** Die empfohlene Standardeinstellung. Ihre E-Mail-Nachrichten werden automatisch und transparent geschützt. Die PGP Corporation empfiehlt, diese Option ausgewählt zu lassen, sofern Sie nicht zur Verwendung der manuellen Proxyeinstellung aufgefordert werden.
- **Manueller Proxy:** Diese Option wird benötigt, wenn Sie eine SSH-Tunnelverbindung zu Ihrem E-Mail-Server verwenden oder wenn der Computer, auf dem PGP Desktop ausgeführt wird, gleichzeitig als E-Mail-Server dient. Weitere Informationen finden Sie unter *Manuellen Modus konfigurieren* (auf Seite 338).

Registerkarte „Instant Messaging“



Wenn der Computer durch eine Netzwerk-Firewall geschützt wird, müssen Sie u. U. den Netzwerkport ändern, der von AIM für Instant Messaging-Sitzungen verwendet wird. Die meisten Benutzer müssen diese Einstellung nicht ändern.

- **Manuellen Proxy verwenden:**Aktivieren Sie dieses Kontrollkästchen, um den Port zu ändern, der von AIM für Instant Messaging-Sitzungen verwendet wird. Geben Sie einen Wert ein, der nicht dem Standardport (5190) entspricht. Erkundigen Sie sich beim Netzwerkadministrator, ob Sie die Einstellung ändern müssen und welcher Port in diesem Fall festgelegt werden muss.

Manuellen Modus konfigurieren

Wenn Sie die manuelle Option für den E-Mail-Proxy **auswählen, müssen Sie auch die PGP Messaging-Einstellungen konfigurieren sowie bestimmte Einstellungen des E-Mail-Clients (die entsprechenden Werte erfahren Sie vom Systemadministrator):**

1. Wählen Sie im Bedienfeld „PGP-Messaging“ den Dienst aus, für den Sie den manuellen Modus verwenden möchten. Das Fenster „Neuer Dienst“ wird angezeigt.
2. Klicken Sie auf **Servereinstellungen**. Das Dialogfeld „Servereinstellungen“ wird für den angegebenen Dienst angezeigt.
3. Wählen Sie den Servertyp für den neuen Dienst aus:
   - **Internet-E-Mail**: Für Benutzer, die PGP Desktop als eigenständige Lösung mit einer POP- oder IMAP-Verbindung nutzen.
   - **PGP Universal**: Für Benutzer von PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung. Wenden Sie sich an den PGP Universal Server-Administrator, wenn Sie weitere Informationen zu diesen Einstellungen benötigen.

- **MAPI/Exchange**: Für Benutzer von PGP Desktop mit Microsoft Outlook als Client auf einem Microsoft Exchange/MAPI-Server. Wenden Sie sich an den E-Mail-Administrator, wenn Sie weitere Informationen zu diesen Einstellungen benötigen.
- **Lotus Notes**: Für Benutzer von PGP Desktop mit Lotus Notes als E-Mail-Client auf einem Lotus Domino-Server. Wenden Sie sich an den E-Mail-Administrator, wenn Sie weitere Informationen zu diesen Einstellungen benötigen.

4 Geben Sie im Bereich **Mailserver für eingehende Nachrichten** im Feld zum Umleiten des lokalen Ports X an einen Server **einen Wert ein.**

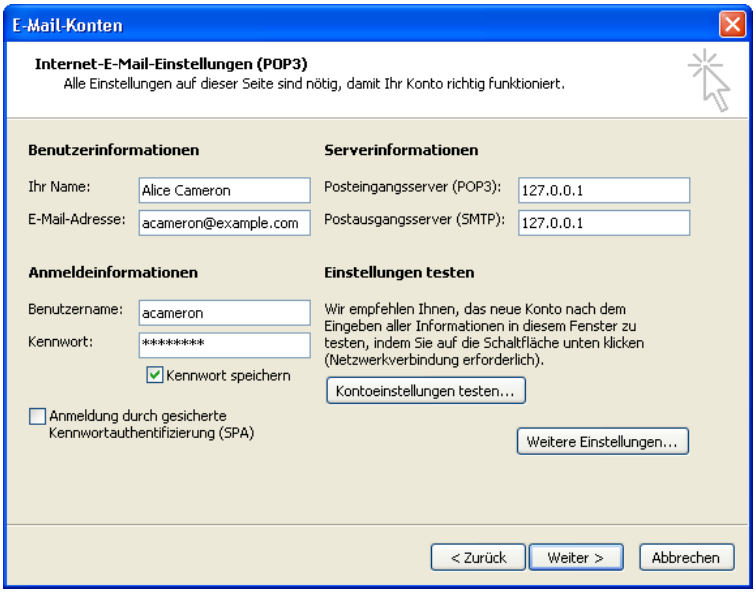
PGP Desktop prüft dann diesen Port auf E-Mail-Nachrichten, die vom E-Mail-Server zum E-Mail-Client gesendet werden.

5 Geben Sie im Bereich **Postausgangsserver (SMTP)** einen Wert im Feld zum Umleiten des lokalen Ports X an einen Server **ein.**

PGP Desktop prüft dann diesen Port auf E-Mail-Nachrichten, die vom E-Mail-Client zum E-Mail-Server gesendet werden.

6 Klicken Sie auf **OK**. Das Dialogfeld „Servereinstellungen“ wird geschlossen.

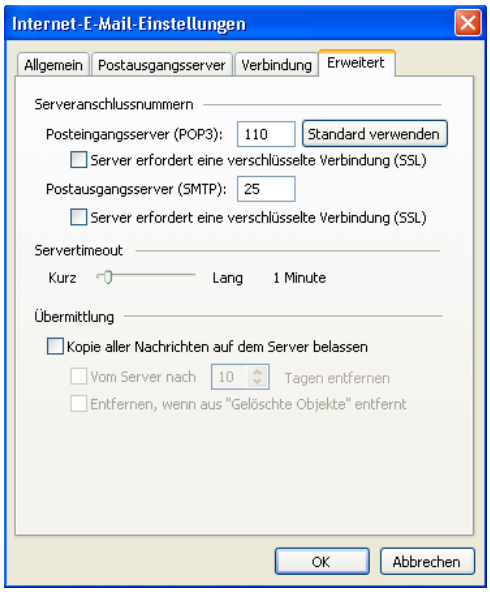
7 Öffnen Sie den E-Mail-Client und wechseln Sie zu den Einstellungen für das E-Mail-Konto (falls Sie mehrere Konten besitzen, müssen Sie jedes Konto einzeln konfigurieren).



8 Geben Sie in Microsoft Outlook für die Einstellungen **Posteingangsserver (POP3)** bzw. **Posteingangsserver (IMAP)** sowie für **Postausgangsserver (SMTP)** den Wert **127.0.0.1** ein.

9 Klicken Sie auf **Weitere Einstellungen**.

10 Klicken Sie im Dialogfeld „Internet-E-Mail-Einstellungen“ auf **Erweitert**. Die Registerkarte **Erweitert** des Dialogfelds „Internet-E-Mail-Einstellungen“ wird angezeigt.



11 Geben Sie in das Feld **Posteingangsserver** (POP3 oder IMAP) den gleichen Wert ein, den Sie für den Server für *eingehende* E-Mail-Nachrichten im Feld zum Umleiten des lokalen Ports X an diesen Server in Schritt 7 dieses Verfahrens festgelegt haben.

12 Geben Sie in das Feld **Postausgangsserver (SMTP)** den gleichen Wert ein, den Sie für den Server für *ausgehende* E-Mail-Nachrichten im Feld zum Umleiten des lokalen Ports X an diesen Server in Schritt 8 dieses Verfahrens festgelegt haben.

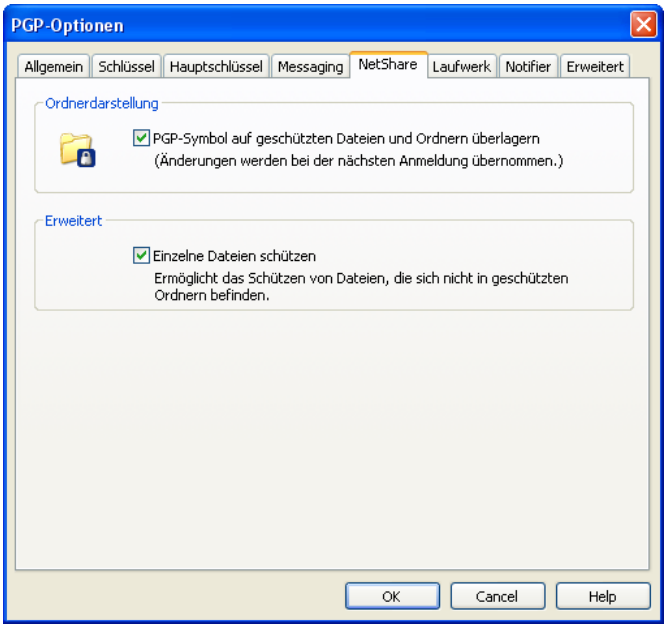
13 Klicken Sie auf **OK** und schließen Sie die Konfiguration der Kontoeinstellungen ab. Der manuelle Modus ist für den ausgewählten Dienst konfiguriert.

14 Wenn Sie mit der Konfiguration des manuellen Modus für die Dienste fertig sind, starten Sie das System neu.

PGP NetShare-Optionen

Verwenden Sie in den Optionen die Registerkarte „NetShare“, um Einstellungen für den Schutz von freigegebenen Netzwerkdateien zu ändern.

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung verwenden, hat Ihr PGP Universal Server-Administrator ggf. bestimmte Funktionen deaktiviert. Ist eine Funktion deaktiviert, wird das Bedienelement auf der linken Seite nicht angezeigt und das Menü oder andere auf diese Funktion zutreffenden Optionen sind nicht verfügbar. Die in diesem Handbuch enthaltenen Abbildungen entsprechen der Standardinstallation, bei der alle Funktionen aktiviert sind. Wenn Ihr PGP Universal Server-Administrator diese Funktion deaktiviert hat, ist dieser Abschnitt für Sie nicht relevant.



- **Ordnerdarstellung:** Wählen Sie die Option **PGP-Symbol auf geschützten Dateien und Ordnern überlagern** aus, wenn ein kleines PGP-Schlosssymbol auf den Dateien und Ordnern angezeigt werden soll, die durch PGP NetShare geschützt sind.
- **Erweitert:** Wählen Sie **Einzelne Dateien schützen** aus, um mit PGP NetShare einzelne Dateien zu schützen, die sich außerhalb eines geschützten Ordners befinden.

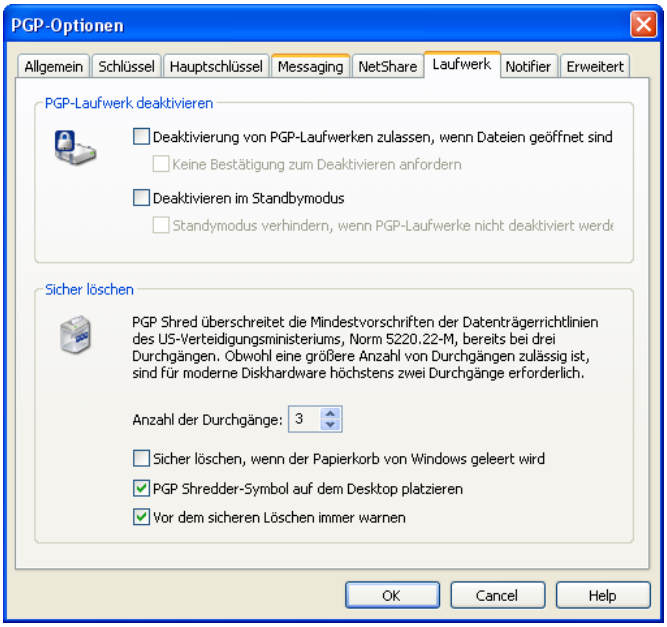
  Hinweis: Der PGP-Administrator hat diese Option u. U. deaktiviert, wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung verwenden.

Weitere Informationen zum Schützen einzelner Dateien außerhalb eines geschützten Ordners mit PGP NetShare finden Sie unter *Dateien außerhalb eines geschützten Ordners schützen* (auf Seite 277).

Laufwerksoptionen

Die Registerkarte „Laufwerk“ enthält Einstellungen für Laufwerke, die mit PGP Virtual Disk geschützt sind. Zudem umfasst die Registerkarte „Laufwerk“ Optionen für PGP Shredder.

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung verwenden, hat Ihr PGP Universal Server-Administrator ggf. bestimmte Funktionen deaktiviert. Ist eine Funktion deaktiviert, wird das Bedienelement auf der linken Seite nicht angezeigt und das Menü oder andere auf diese Funktion zutreffenden Optionen sind nicht verfügbar. Die in diesem Handbuch enthaltenen Abbildungen entsprechen der Standardinstallation, bei der alle Funktionen aktiviert sind. Wenn Ihr PGP Universal Server-Administrator diese Funktion deaktiviert hat, ist dieser Abschnitt für Sie nicht relevant.


PGP-Optionen
Allgemein
Schlüssel
Hauptschlüssel
Messaging
NetShare
Laufwerk
Notifier
Erweitert
PGP-Laufwerk deaktivieren
Deaktivierung von PGP-Laufwerken zulassen, wenn Dateien geöffnet sind
Keine Bestätigung zum Deaktivieren anfordern
Deaktivieren im Standbymodus
Standymodus verhindern, wenn PGP-Laufwerke nicht deaktiviert werde
Sicher löschen
PGP Shred überschreitet die Mindestvorschriften der Datenträgerrichtlinien des US-Verteidigungsministeriums, Norm 5220.22-M, bereits bei drei Durchgängen. Obwohl eine größere Anzahl von Durchgängen zulässig ist, sind für moderne Diskhardware höchstens zwei Durchgänge erforderlich.
Anzahl der Durchgänge: 3
Sicher löschen, wenn der Papierkorb von Windows geleert wird
PGP Shredder-Symbol auf dem Desktop platzieren
Vor dem sicheren Löschen immer warnen
OK
Cancel
Help

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, sind diese Optionen möglicherweise bereits konfiguriert.

PGP-Laufwerk deaktivieren

Folgende Optionen sind für PGP Virtual Disk verfügbar:

- **Deaktivierung von PGP-Laufwerken zulassen, wenn Dateien geöffnet sind:** In der Regel kann ein PGP Virtual Disk-Laufwerk nicht automatisch deaktiviert werden, wenn auf dem Laufwerk Dateien geöffnet sind. Wenn diese Option aktiviert ist, kann das Laufwerk auch mit geöffneten Dateien deaktiviert werden (auch als erzwungene Deaktivierung bezeichnet).
  - **Keine Bestätigung zum Deaktivieren anfordern**: Ermöglicht PGP Desktop, die Deaktivierung eines PGP Virtual Disk-Laufwerks zu erzwingen, *ohne* zuvor eine Warnung anzuzeigen, dass möglicherweise Dateien geöffnet sind.

Warnung: Falls Sie die Deaktivierung eines PGP Virtual Disk-Laufwerks erzwingen, während Dateien geöffnet sind, könnten Daten verloren gehen.

- **Deaktivieren im Standbymodus:** Wenn diese Option ausgewählt ist, deaktiviert PGP Desktop automatisch alle aktivierten PGP Virtual Disk-Laufwerke, sobald der Computer in einen Standby- oder Ruhemodus wechselt.
  - Wählen Sie die Option **Standbymodus verhindern, wenn PGP-Laufwerke nicht deaktiviert werden können** aus, um zu verhindern, dass der Computer in den Standbymodus wechselt, wenn ein PGP Virtual Disk-Laufwerk nicht deaktiviert werden kann. Diese Option ist unter Microsoft Windows Vista nicht verfügbar (Windows Vista ermöglicht das Verhindern des Standbymodus nicht mehr).

Warnung: Der Ruhezustand von Windows ist nicht sicher, da Windows vertrauliche Daten auf den Datenträger schreibt, wenn das PGP Virtual Disk-Laufwerk beim Aktivieren des Ruhezustands geöffnet ist. Die PGP Corporation empfiehlt, eine Verschlüsselung mit PGP Whole Disk Encryption durchzuführen, wenn Sie den Ruhezustand verwenden. Andernfalls sollten Sie die Optionen **Deaktivieren im Standbymodus** und **Stromsparmodus verhindern, falls PGP-Laufwerke nicht deaktiviert werden können** aktivieren.

Sicher löschen

Mit PGP Shredder können Sie vertrauliche Daten sicher löschen. Sie können die Sicherheitsstufe von PGP Shredder sowie andere Einstellungen anpassen.

PGP Shredder bietet folgende Optionen:

- **Anzahl der Durchgänge:** PGP Shredder entfernt die Dateien sicher, indem sie normal gelöscht werden. Dann wird der Speicherplatz, der zuvor von den soeben gelöschten Dateien belegt war, mit Nullen überschrieben.

  Mit diesem Verfahren können Dateien in nur wenigen Durchgängen sehr sicher gelöscht werden. Daher sind standardmäßig **3** Durchgänge vorgesehen, die ein äußerst hohes Maß an Sicherheit bieten. Sie können die gewünschte Sicherheitsstufe jedoch noch steigern, indem Sie diese Einstellung Ihren Bedürfnissen entsprechend auf bis zu 49 Durchgänge erhöhen.

Beachten Sie dabei, dass die zusätzliche Sicherheit mit einem erhöhten Zeitaufwand für das sichere Löschen der Dateien verbunden ist. Der Zeitaufwand ist von mehreren Faktoren abhängig, insbesondere jedoch von der Geschwindigkeit des Prozessors.

Folgende Richtlinien werden für die Anzahl der Durchgänge empfohlen:

- 3 Durchgänge für den persönlichen Gebrauch
- 10 Durchgänge für den kommerziellen Gebrauch
- 18 Durchgänge für den militärischen Gebrauch
- 26 Durchgänge für maximale Sicherheit

- **Sicher löschen, wenn der Papierkorb von Windows geleert wird:** Aktivieren Sie dieses Kontrollkästchen, wenn der Inhalt des Windows-Papierkorbs bei jedem Leeren sicher von PGP Shredder gelöscht werden soll. Verwenden Sie diese Option mit Vorsicht, da alle im Papierkorb vorhandenen Dateien sicher von PGP Shredder gelöscht werden. Dies schließt auch nicht vertrauliche Dateien ein. Bei großen Dateien kann der Vorgang u. U. länger dauern.

  Mit dieser Option werden auch Dateien automatisch sicher gelöscht, die Sie unter Umgehung des Papierkorbs löschen (indem Sie beim Löschen der Elemente die Umschalttaste gedrückt halten). Darüber hinaus werden temporäre System- und Anwendungsdateien sicher gelöscht, die automatisch vom System gelöscht werden.

  Bei dieser automatischen Datenvernichtung werden dieselben von Ihnen ausgewählten Einstellungen für PGP Shredder verwendet, die auch für das manuelle sichere Löschen gelten.

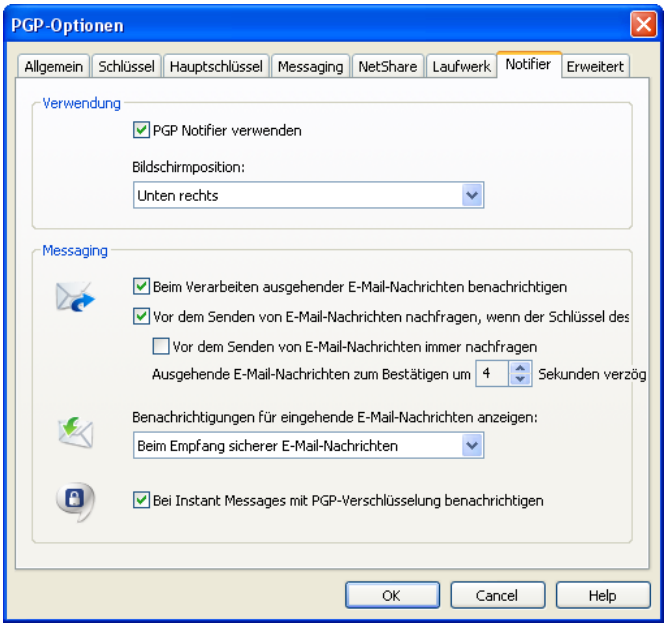
- **PGP Shredder-Symbol auf dem Desktop platzieren**: Aktivieren Sie dieses Kontrollkästchen, wenn ein Symbol für PGP Shredder auf dem Desktop angelegt werden soll. Sie können dieses Symbol auf die gleiche Art wie das Symbol des Windows-Papierkorbs verwenden und Dateien einfach auf das Symbol ziehen. Diese Option ist standardmäßig aktiviert.

- **Vor dem sicheren Löschen immer warnen**:Aktivieren Sie dieses Kontrollkästchen, wenn vor jedem sicheren Löschvorgang ein Bestätigungsdialogfeld angezeigt werden soll. Dadurch können Sie noch einmal überprüfen, ob wirklich nur die gewünschten Dateien sicher gelöscht werden. Diese Option ist standardmäßig aktiviert.

Tipp: Daten können u. U. auch an anderen Speicherorten abgelegt sein, z. B. in temporären Dateien. Aus diesem Grund sollten Sie PGP Whole Disk Encryption verwenden, um alle Daten auf dem System zu schützen.

Notifier-Optionen

Auf der Registerkarte **Notifier** finden Sie Einstellungen für die Notifier-Funktion von PGP Desktop. Der Notifier zeigt Statusmeldungen in einer Ecke des Bildschirms an, wenn Sie E-Mail-Nachrichten senden oder empfangen. Darüber hinaus wird der Status angezeigt, wenn Sie PGP Whole Disk Encryption und PGP NetShare verwenden.



Weitere Informationen zur Notifier-Funktion von PGP Desktop finden Sie unter *Notifier-Warnungen von PGP Desktop* (auf Seite 36).

Verwendungsoptionen

- Aktivieren Sie Benachrichtigungen, indem Sie **PGP Notifier verwenden** und dann eine Option unter **Bildschirmposition** auswählen.
- **Bildschirmposition:** PGP Desktop-Benachrichtigungen können in einer der vier Ecken des Bildschirms angezeigt werden (**Unten rechts**, **Unten links**, **Oben rechts** oder **Oben links**). Wählen Sie die Ecke aus, in der die PGP Desktop-Benachrichtigungen angezeigt werden sollen. Die Standardposition ist **Unten rechts**.

Messaging-Optionen

Folgende Einstellungen sind für die Notifier-Funktion von PGP Desktop verfügbar:

- **Beim Verarbeiten ausgehender E-Mail-Nachrichten benachrichtigen:** Aktivieren Sie dieses Kontrollkästchen, wenn beim Senden von E-Mail-Nachrichten Notifier-Meldungen von PGP Desktop mit Informationen zum Verschlüsselungs- und/oder Signierstatus angezeigt werden sollen. Deaktivieren Sie dieses Kontrollkästchen, wenn Sie beim Senden von E-Mail-Nachrichten keine PGP Desktop-Benachrichtigungen wünschen.
- **Vor dem Senden von E-Mail-Nachrichten nachfragen, wenn der Schlüssel des Empfängers nicht gefunden wird:** PGP Desktop sucht nach einem öffentlichen Schlüssel für jeden Empfänger der von Ihnen gesendeten E-Mail-Nachrichten. Wenn für einen Empfänger kein öffentlicher Schlüssel gefunden werden kann, wird die betreffende E-Mail-Nachricht standardmäßig als Klartext (ohne Verschlüsselung) gesendet. Wenn Sie diese Notifier-Option auswählen, werden Sie in solchen Fällen benachrichtigt und erhalten die Möglichkeit, die betreffende E-Mail-Nachricht zu blockieren, damit sie nicht gesendet wird.

  (Weitere Informationen zu den Einstellungen für die Standardrichtlinien von PGP Desktop finden Sie unter *Dienste und Richtlinien* (auf Seite 103).)

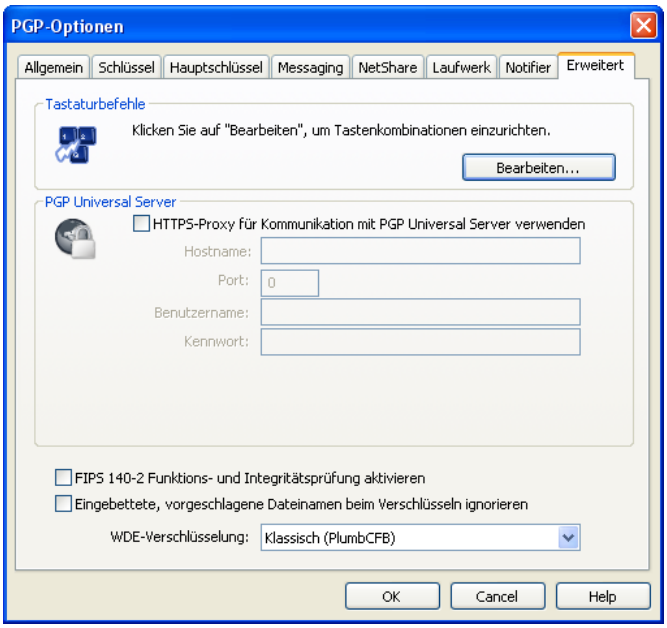
  - **Vor dem Senden von E-Mail-Nachrichten immer nachfragen:** Aktivieren Sie dieses Kontrollkästchen, wenn Sie jede E-Mail-Nachricht vor dem Versand bestätigen möchten. Sie können den Verschlüsselungsstatus im Notifier-Fenster überprüfen und dann entscheiden, ob die E-Mail-Nachricht gesendet oder blockiert werden soll.
  - **Ausgehende E-Mail-Nachricht zum Bestätigen um n Sekunden verzögern** (wobei *n* für eine Zahl zwischen 1 und 30 steht; der Standardwert beträgt 4 Sekunden): Ändern Sie die Verzögerungszeit für ausgehende Nachrichten sowie die Zeit für die Anzeige des Notifier-Fensters von PGP Desktop, indem Sie die Pfeiltasten nach oben und nach unten verwenden. Innerhalb der Verzögerungszeit können Sie die Notifier-Meldung von PGP Desktop überprüfen.
- **Benachrichtigungen für eingehende E-Mail-Nachrichten anzeigen:** Geben Sie für eingehende E-Mail-Nachrichten an, in welchem Umfang Sie beim Empfang einer E-Mail-Nachricht über deren Status informiert werden möchten. Folgende Optionen sind verfügbar:
  - **Beim Empfang sicherer E-Mail-Nachrichten**: Beim Empfang sicherer E-Mail-Nachrichten wird ein Notifier-Fenster angezeigt. Dieses Fenster enthält den Absender der E-Mail-Nachricht, den Betreff, den Verschlüsselungs- sowie den Verifizierungsstatus und die E-Mail-Adresse des Absenders.
  - **Nur beim Fehlschlagen der Nachrichtenüberprüfung**: Eine Notifier-Meldung wird nur dann für eingehende E-Mail-Nachrichten angezeigt, wenn PGP Desktop die Signatur der eingehenden E-Mail-Nachricht nicht verifizieren kann.

- **Nie**: Wählen Sie diese Option aus, wenn beim Empfang von E-Mail-Nachrichten keine Notifier-Meldung angezeigt werden soll. Diese Option wirkt sich nicht auf Notifier-Meldungen für ausgehende E-Mail-Nachrichten aus.

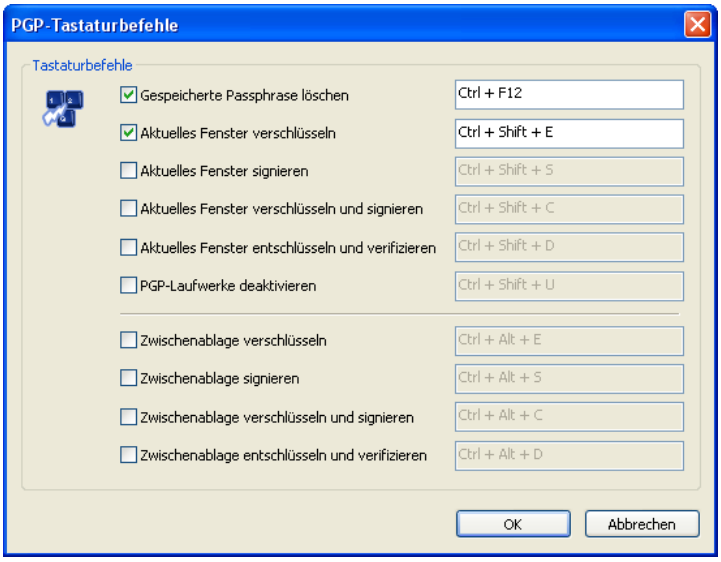
- **Bei Instant Message-Konversationen mit PGP-Verschlüsselung benachrichtigen**: Aktivieren Sie dieses Kontrollkästchen, wenn zu Beginn und bei Beendigung eines sicheren Instant Messaging-Chats kurz eine Notifier-Meldung von PGP Desktop angezeigt werden soll.

Erweiterte Optionen

Auf der Registerkarte mit den erweiterten PGP-Optionen können sehr spezifische Einstellungen festgelegt werden. Die meisten Benutzer müssen diese Einstellungen nicht ändern.



- **Tastaturbefehle**: In PGP Desktop stehen Ihnen viele Möglichkeiten zur Verfügung, benutzerdefinierte Tastaturbefehle zu definieren, um schneller und einfacher zu arbeiten. In PGP Desktop sind bereits zahlreiche Tastaturbefehle vorkonfiguriert, Sie können die Tastenbelegungen jedoch nach Ihren Bedürfnissen ändern. Klicken Sie auf **Bearbeiten**, um das Dialogfeld „PGP-Tastaturbefehle“ anzuzeigen.



- **PGP Universal: HTTPS-Proxy für Kommunikation mit PGP Universal verwenden:** Ändern Sie diese Einstellungen nur, wenn Sie vom Netzwerkadministrator dazu aufgefordert werden.

  Wenn für Ihre Installation von PGP Universal Server eine sichere Client-Server-Verbindung über einen Proxy erforderlich ist, können Sie dies über diese Einstellungen angeben. Informationen zu Servername, verwendetem Kommunikationsport, Benutzer-ID und Kennwort zur ordnungsgemäßen Konfiguration dieses Abschnitts erhalten Sie vom Administrator.

- Ändern Sie einen Schlüssel (oder den Schlüsselmodus), indem Sie auf **Schlüssel zurücksetzen** klicken. Weitere Informationen zu Schlüsselmodi finden Sie unter *Schlüsselmodi* (auf Seite 136). Diese Option ist verfügbar, wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen.

- **FIPS 140-2 Funktions- und Integritätsprüfung aktivieren:** Wählen Sie diese Option aus, wenn von Ihnen oder von Ihrer Organisation Überprüfungen nach FIPS 140-2 durchgeführt werden sollen. Beachten Sie jedoch, dass die Computerleistung dadurch beeinträchtigt wird. Sie müssen den Computer neu starten, damit diese Einstellung übernommen wird.

- **Eingebettete, vorgeschlagene Dateinamen beim Verschlüsseln ignorieren**: Wählen Sie diese Option aus, um Empfehlungen zu ignorieren, die von PGP Desktop beim Verschlüsseln von Dateien ausgegeben werden.

  Wenn Sie PGP Desktop Version 8.1 mit einer internationalen Einstellung (z. B. Japan) verwenden, verschlüsselt PGP Desktop den vorgeschlagenen Dateinamen nicht richtig. Diese Einstellung muss aktiviert sein, um eine ordnungsgemäße Kommunikation zwischen PGP Desktop 8.1 und 9.x sicherzustellen, wenn Dateien in PGP Desktop 9.x entschlüsselt werden, die mit PGP Desktop 8.1 verschlüsselt wurden.

B Mit Kennwörtern und Passphrasen arbeiten

Kennwörter und Passphrasen werden verwendet, um Informationen zu schützen. Passphrases, wörtlich übersetzt Schlüsselsätze, sind länger als Kennwörter und können mehrere Wörter und eine breitere Palette an Zeichen verwenden. Da der Ausdruck „Passphrase“ im Deutschen nicht sehr gebräuchlich oder verständlich ist, wird in diesem PGP-Produkt zum leichteren Verständnis der Ausdruck Passphrase verwendet. Sie können als Passphrase aber auch ganze Sätze verwenden. Sie erreichen dadurch eine höhere Sicherheit als mit einfachen Kennwörtern.

Ein Beispiel für ein einfaches Kennwort ist ein Wort mit vier Buchstaben oder zwei zusammenhängende Worte: „wennarbeit“ ohne die Anführungszeichen. Ein stärkeres Kennwort beinhaltet außerdem Großbuchstaben: WennArbeit. Noch besser ist es, wenn Sie Ziffern hinzufügen: Wenn9Arbeit4.

Im Vergleich hierzu sind Passphrasen länger und verwenden eine breitere Palette von Zeichen. Eine einfache Passphrase ist zum Beispiel: „Mb&iw>8aG.“ (ohne Anführungszeichen, aber mit Punkt). Diese Passphrase scheint zwar auf den ersten Blick schwer merkbar zu sein, da sie jedoch auf einem einfachen Satz basiert, lässt sie sich leichter merken.

Passphrasen können auch aus einfachen Sätzen bestehen, z. B. aus einem Buch, einschließlich der Satzzeichen und Groß-/Kleinschreibung. „Weil das nicht Golf ist, antwortete ich“ (einschließlich Anführungszeichen). Obwohl dies nicht nach einer starken Passphrase aussieht, ist es doppelt so stark wie die bisherigen Beispiele.

In diesem Abschnitt werden die Unterschiede zwischen Kennwörtern und Passphrasen beschrieben. Zudem finden Sie hier Informationen zur Passphrasen-Qualitätsanzeige in PGP Desktop sowie Richtlinien zum Erstellen starker Passphrasen.

In diesem Kapitel

Entscheidung über die Verwendung eines Kennwortes oder einer Passphrase 352
Die Passphrasen-Qualitätsanzeige 352
Starke Passphrasen erstellen 353
Vorgehensweise bei vergessenen Passphrasen 355

Entscheidung über die Verwendung eines Kennwortes oder einer Passphrase

Wie entscheiden Sie, ob Sie ein Kennwort oder eine Passphrase verwenden sollten? Das hängt davon ab, was Sie schützen möchten. Je wertvoller die Informationen sind, die Sie schützen möchten, desto stärker sollte der Schutz sein.

Die meisten Word-Dokumente sind überhaupt nicht geschützt. Ihr Inhalt ist nicht wichtig genug, damit der Aufwand gerechtfertigt ist. Für Ihr Online-Banking benötigen Sie bereits mindestens eine vierstellige PIN. Abhängig von Ihrem Kontostand stellt das ein sehr hohes oder sehr niedriges Sicherheitsniveau dar. Für Ihre unwichtige Korrespondenz verwenden Sie vielleicht ein Hotmail-Konto. Ein einfaches Kennwort ist hierfür ausreichend. Für das E-Mail-Konto an Ihrem Arbeitsplatz, über das Sie interne Produkt-, Kunden- und Buchhaltungsinformationen erhalten, sollten Sie ein starkes Kennwort verwenden.

Mit PGP Desktop können Sie beispielsweise eine Passphrase für Ihr PGP-Schlüsselpaar und für Ihre PGP Virtual Disk-Laufwerke erstellen. Wenn Sie für Ihr PGP-Schlüsselpaar nur eine schwache Passphrase verwenden und ein Angreifer physischen Zugriff auf die private Schlüsseldatei hat, muss er lediglich die Passphrase herausfinden, um die Nachrichten, die Sie senden und empfangen, lesen zu können.

Die Passphrasen-Qualitätsanzeige

Beim Erstellen von Passphrasen in PGP Desktop kann die Passphrasen-Qualitätsanzeige als allgemeiner Anhaltspunkt für die Stärke der erstellten Passphrase verwendet werden. Auf jeden Fall handelt es sich um einen besseren Anhaltspunkt als lediglich die Anzahl der Zeichen.

Je länger die Anzeige, desto stärker ist im Allgemeinen die Passphrase. Was bedeutet die Länge der Passphrasen-Qualitätsanzeige jedoch wirklich?

Die Passphrasen-Qualitätsanzeige vergleicht die Zufallsmenge (Entropiewert) der von Ihnen eingegebenen Passphrase mit einer echten zufälligen Zeichenkette mit 128 Bit (was dem Entropiewert eines AES-128-Schlüssels entspricht). Dies wird als Entropie von 128 Bit bezeichnet.

(Entropie ist ein Maßstab für den Schwierigkeitsgrad beim Festlegen eines Kennworts oder eines Schlüssels.)

Wenn die von Ihnen erstellte Passphrase die Passphrasen-Qualitätsanzeige ungefähr halb ausfüllt, verfügt diese Passphrase über eine Entropie von etwa 64 Bit. Wenn die Passphrase die Passphrasen-Qualitätsanzeige komplett ausfüllt, weist diese Passphrase einen Entropie von etwa 128 Bit auf.

Wie stark ist demnach eine Entropie von 128 Bit? Ende der 90er Jahre wurden spezialisierte „DES-Cracker"-Computer gebaut, die innerhalb weniger Stunden durch Ausprobieren aller möglichen Schlüsselwerte einen DES-Schlüssel herausfinden konnten.

Wenn Sie einen Computer bauen könnten, der innerhalb einer Sekunde einen DES-Schlüssel herausfinden kann (der Computer müsste in der Lage sein, 255 Schlüssel pro Sekunde auszuprobieren), würde der Computer ca. 149 Billionen (Tausend Milliarden) Jahre benötigen, um einen AES-Schlüssel von 128 Bit herauszufinden. Im Vergleich dazu soll das Universum nicht einmal 20 Milliarden Jahre alt sein.

Wie wird die Entropie eines bestimmten Zeichens gemessen? Je größer die Menge von Zeichen ist, aus dem ein bestimmtes Zeichen ausgewählt werden kann, desto mehr Entropie wird dem ausgewählten Zeichen zugewiesen.

Wenn Sie beispielsweise eine numerische PIN auswählen sollen, beschränkt sich die Auswahl auf die Zahlen Null bis Neun, also insgesamt 10 Zeichen. Die Menge ist also recht klein und die Entropie für das ausgewählte Zeichen ist relativ gering.

Wenn Sie eine Passphrase mithilfe der englischen Version von PGP Desktop auswählen, ist die Sachlage jedoch anders. Sie können aus drei Mengen von Zeichen auswählen: Großbuchstaben und Kleinbuchstaben (52 Zeichen), den Zahlen Null bis Neun (10 Zeichen) und den Interpunktionszeichen auf einer Standardtastatur (32 Zeichen).

PGP Desktop bestimmt beim Eingeben eines Zeichens den Entropiewert für das jeweilige Zeichen basierend auf der Menge von Zeichen, der es angehört. Dieser Wert wird auf die Passphrasen-Qualitätsanzeige angewendet.

Das gleiche Konzept gilt für die Zeichensätze anderer Sprachen. Je größer die Datenbasis, desto mehr Entropie pro Zeichen. Wenn Sie z. B. einen asiatischen oder arabischen Zeichensatz verwenden, von denen manche über mehrere Hundert Zeichen verfügen, wäre die Entropie für ein ausgewähltes Zeichen entsprechend höher und die Passphrasen-Qualitätsanzeige würde wesentlich schneller ausgefüllt.

Starke Passphrasen erstellen

Beim Erstellen einer guten Passphrase wird in der Regel ein Kompromiss zwischen Benutzerfreundlichkeit und Stärke der Passphrase eingegangen. Längere Passphrasen mit Groß- und Kleinbuchstaben, Zahlen sowie Interpunktionszeichen sind zwar stärker, jedoch auch schwieriger zu merken.

Untersuchungen haben gezeigt, dass schwieriger zu merkende Passphrasen häufiger aufgeschrieben werden, was jedoch den Sinn einer starken Passphrase verfehlt. Es ist daher besser, eine kürzere starke Passphrase zu verwenden, die Sie sich merken können, als eine längere starke Passphrase, die Sie sich aufschreiben, um sie nicht zu vergessen.

Oft wird beim Erstellen von starken Passphrasen ein Ausdruck zu einzelnen Zeichen verkürzt. Als Beispiel wird folgender Ausdruck herangezogen:

```
Mein Bruder und ich wollen größere Acht aufeinander
geben.
```

Daraus ergibt sich folgende Passphrase:

```
Mb&iw>8aG.
```

Diese Passphrase besteht aus 10 Zeichen und enthält Groß- und Kleinbuchstaben, Zahlen sowie Interpunktionszeichen. Mit 10 Zeichen handelt es sich hierbei um eine relativ kurze Passphrase. Wenn 10 Zeichen Ihrer Meinung nach nicht ausreichen, können Sie entweder mit derselben Methode eine weitere Passphrase erstellen und dann beide zusammen verwenden oder einfach mit einem längeren Ausdruck beginnen.

Bei einer anderen Methode werden einfache Ausdrücke mit Interpunktionszeichen und Großbuchstaben verwendet. Beispiel:

```
Editiert von John Doe (nicht John Doe, Editor)
```

Hierbei handelt es sich um eine starke Passphrase, obwohl sie nicht besonders lang oder kompliziert ist. Wenn Sie einen Ausdruck aus einem Ihnen bekannten Buch verwenden, dürfen Sie das Buch nicht verlieren.

Sie können beim Erstellen einer Passphrase in PGP Desktop bis zu 255 Zeichen, einschließlich Leerzeichen, verwenden.

Ein weiterer Ansatz ist das Verknüpfen vieler kurzer, gängiger Wörter. Bei einer als Diceware™ bezeichneten Methode werden Würfel verwendet, um aus einer besonderen Liste, der Diceware Word List, die 7776 kurze englische Wörter, Abkürzungen und leicht zu merkende Zeichenketten enthält, zufällige Wörter auszuwählen. Wenn Sie eine ausreichende Anzahl dieser Zeichenketten zusammenfügen, können Sie eine starke Passphrase erstellen. In den häufig gestellten Fragen von Diceware wird angegeben, dass mit einer Passphrase aus 10 Diceware-Wörtern Entropie von 128 Bit erzielt werden kann.

Weitere Informationen zu Diceware finden Sie auf der *Diceware Passphrase-Website* (http://world.std.com/~reinhold/diceware.html).

Beachten Sie bei der Erstellung von Passphrasen Folgendes:

- Verwenden Sie eine Passphrase aus Ihrem Langzeitgedächtnis. Dadurch reduzieren Sie die Gefahr, dass Sie sie vergessen.
- Achten Sie darauf, dass die Passphrase mindestens acht Zeichen umfasst. Obwohl die Länge nicht mit der Stärke gleichzusetzen ist, ist eine lange Passphrase besser als eine kurze.
- Verwenden Sie Groß- und Kleinbuchstaben, Zahlen sowie Interpunktionszeichen.

Achtung: Verwenden Sie nach Möglichkeit nur ASCII-Zeichen. Dies ist besonders wichtig, wenn Sie internationale Tastaturen verwenden, da bestimmte Sonderzeichen (z. B. §) in Passphrasen nicht unterstützt werden.

- Ändern Sie die Passphrase regelmäßig, beispielsweise alle drei Monate. Je länger Sie dieselbe Passphrase verwenden, desto mehr Zeit geben Sie anderen, diese ausfindig zu machen.

Folgendes sollten Sie beim Erstellen von Passphrasen **vermeiden**:

- Schreiben Sie Ihre Passphrase nicht auf.
- Verraten Sie Ihre Passphrase niemals anderen Personen.
- Lassen Sie sich beim Eingeben der Passphrase nicht beobachten.
- Verwenden Sie nicht die Begriffe „Passwort“, „Kennwort“ oder „Passphrase“.
- Verwenden Sie keine Muster. Also nicht „abcdefgh“ oder „12345678“ oder „qwertzui“ oder „88888888“ oder „AAAAAAAA“.
- Verwenden Sie keine gebräuchlichen Wörter. Fast alle Hacker mit Erfahrung verwenden ein Wörterbuch zum Knacken von Kennwörtern, bei dem geläufige Wörter versucht werden. Verketten Sie nicht zwei gebräuchliche Wörter, verwenden Sie nicht die Pluralform eines geläufigen Wortes und verwenden Sie kein geläufiges Wort mit einem großen Anfangsbuchstaben.
- Verwenden Sie keine Zahlen, die sich auf Sie beziehen. Wenn jemand diese Zahlen kennt, könnten Hacker sie ausfindig machen. Verwenden Sie auf keinen Fall Ihr Geburtsdatum, Ihre Telefonnummer, Ihre Sozialversicherungsnummer oder Ihre Hausnummer.
- Verwenden Sie keine Namen. Verwenden Sie nicht die Namen von Personen, fiktiven Personen oder den Namen Ihres Haustiers. Verwenden Sie nicht den Namen Ihres letzten Urlaubsorts, Ihren Anmeldenamen oder den Namen Ihres Unternehmens. Verwenden Sie nicht den Namen Ihrer Lieblingsmannschaft oder eines Körperteils. Verwenden Sie außerdem keine Namen aus Büchern, insbesondere aus der Bibel.
- Verwenden Sie keine der oben genannten Wörter von hinten nach vorne gelesen oder mit einem einzelnen voran- bzw. nachgestellten Zeichen.

Vorgehensweise bei vergessenen Passphrasen

Wenn Sie Ihre Passphrase vergessen, können Sie Informationen, die an Ihren Schlüssel verschlüsselt wurden, nie mehr entschlüsseln. Sie können den Schlüssel jedoch wiederherstellen, wenn der PGP-Administrator eine Richtlinie zur Schlüsselwiederherstellung für Ihr Unternehmen implementiert hat. Weitere Informationen finden Sie unter *PGP-Schlüsselwiederherstellung* (siehe "Schlüssel mit PGP Universal Server wiederherstellen" auf Seite 89, "Vorgehensweise bei verloren gegangenen Schlüsseln oder Passphrasen" auf Seite 89). Sie können sich auch an den PGP-Administrator wenden.

C PGP Desktop mit PGP Universal Server verwenden

Mit PGP Universal Server können Unternehmen E-Mail-Nachrichten anhand konfigurierbarer Richtlinien, die vom PGP-Administrator zur Durchsetzung der Sicherheitsrichtlinien der Organisation erstellt werden, automatisch und (für den Endbenutzer) transparent geschützt werden. PGP Universal ermöglicht PGP-Administratoren darüber hinaus die Verwaltung der Bereitstellung von PGP Desktop an Benutzer innerhalb ihrer Organisation. Weitere Informationen zum PGP Universal Server finden Sie auf der Seite zum *PGP Universal Server auf der PGP-Website* (http://www.pgp.com/products/universal/index.html).

Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, profitieren Sie bis zur Desktop-Ebene von der bewährten PGP-Verschlüsselungstechnologie sowie der weiteren Sicherheitsfunktionen in PGP Desktop, u. a. PGP Whole Disk Encryption, PGP Virtual Disk-Laufwerken, PGP Zip-Archiven und PGP Shredder.

Damit Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen können, müssen Sie PGP Desktop mithilfe eines vom PGP-Administrator erhältlichen Installationsprogramms installieren.

Wenn Sie eine Version von PGP Desktop für den privaten Gebrauch erworben haben und sie nicht in einem Unternehmensumfeld verwenden, haben Sie wahrscheinlich eine eigenständige Version, sodass dieser Abschnitt für Sie nicht relevant ist.

Achtung: Wenn Sie PGP Desktop in einem Unternehmensumfeld verwenden und das Installationsprogramm für PGP Desktop nicht vom PGP-Administrator erhalten haben, wenden Sie sich an den PGP-Administrator, **bevor** Sie diese Version von PGP Desktop installieren oder verwenden.

In diesem Abschnitt werden die Unterschiede bei der Verwendung von PGP Desktop in einer von einem PGP Universal Server verwalteten E-Mail-Domäne beschrieben.

In diesem Kapitel

Übersicht 358
Für PGP-Administratoren 359
Manuelle Bindung an einen PGP Universal Server 359

Übersicht

Das Installationsprogramm von PGP Desktop wurde vom PGP-Administrator auf eine der folgenden Weisen konfiguriert:

- **Keine Richtlinieneinstellungen**: Ihre Kopie von PGP Desktop verfügt nicht über integrierte Einstellungen. Sie können alle Funktionen verwenden, die von der Lizenz unterstützt werden.
- **Automatische Erkennung von Richtlinieneinstellungen**: Ihre Kopie von PGP Desktop wird eine Verbindung zu dem PGP Universal Server herstellen, der das Installationsprogramm erstellt hat, und wird die entsprechenden Einstellungen herunterladen. Aufgrund der erhaltenen Einstellungen müssen Sie Funktionen von PGP Desktop möglicherweise auf eine bestimmte Art und Weise verwenden.
- **Voreingestellte Richtlinieneinstellungen**: Die entsprechenden Einstellungen sind bereits in Ihre Kopie von PGP Desktop integriert. Aufgrund dieser Einstellungen müssen Sie Funktionen von PGP Desktop möglicherweise auf eine bestimmte Art und Weise verwenden.

Da Ihre Kopie von PGP Desktop Einstellungen von einem PGP Universal Server erhält, müssen Sie Funktionen von PGP Desktop möglicherweise auf eine bestimmte Art und Weise verwenden. Dies umfasst Folgendes:

- Möglicherweise müssen Sie bei der Installation von PGP Desktop bestimmte Aktionen ausführen. Es ist beispielsweise möglich, dass Sie das Startlaufwerk mit PGP Whole Disk verschlüsseln oder ein PGP Virtual Disk-Laufwerk erstellen müssen.
- Möglicherweise können oder müssen Sie Funktionen von PGP Desktop auf eine bestimmte Art und Weise verwenden. Eventuell müssen Sie Ihre Instant Messaging-Sitzungen mit AIM verschlüsseln oder Sie können Dateien beim Löschen automatisch sicher löschen.
- Möglicherweise können Sie bestimmte Funktionen von PGP Desktop nicht verwenden. Beispielsweise werden Sie ggf. daran gehindert, konventionelle Verschlüsselung zu verwenden oder selbstentschlüsselnde Archive (SDAs) zu erstellen.
- Möglicherweise müssen Sie bestimmte Messaging-Richtlinien einhalten. Beispielsweise kann es sein, dass Sie Nachrichten an bestimmte E-Mail-Domänen verschlüsseln und signieren müssen.
- Möglicherweise sind bestimmte Funktionen wie PGP Messaging oder PGP NetShare (unter Windows) deaktiviert oder Ihnen wird ein benutzerdefinierter PGP Whole Disk Encryption BootGuard-Bildschirm (unter Windows) angezeigt. Weitere Informationen finden Sie unter *Vom PGP Universal Server-Administrator angepasste Funktionen* (auf Seite 6).

Auf Funktionen von PGP Desktop, die von einem PGP-Administrator in einer von einem PGP Universal Server verwalteten Umgebung verwaltet werden können, wird in ihrer Beschreibung im gesamten Benutzerhandbuch hingewiesen.

Wenden Sie sich an den PGP-Administrator, um weitere Informationen zu den Unterschieden bei der Verwendung von PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung zu erhalten.

Für PGP-Administratoren

Falls Sie als PGP-Administrator die Implementierung von PGP Desktop für manche oder alle Benutzer in Ihrer Organisation verwalten, empfiehlt die PGP Corporation, den PGP Desktop-Benutzern die Verwaltung ihrer eigenen Schlüssel zu überlassen. Dies geschieht mithilfe des Client Key Mode.

Bei der Vorbereitung zur Erstellung der Installationsprogramme von PGP Desktop auf dem PGP Universal Server können Sie bestimmen, ob die PGP Desktop-Benutzer die Möglichkeit erhalten, ihre eigenen Schlüssel zu verwalten (Client Key Mode) oder ob der PGP Universal Server die Schlüsselverwaltung für die Benutzer übernimmt (Server Key Mode).

Diese Einstellungen werden bei der Schlüsseleinrichtung im Standardbildschirm im Bereich für die Schlüsselverwaltung festgelegt, der Teil der Konfiguration der standardmäßigen Benutzergruppenrichtlinie für interne Benutzer ist (**Benutzergruppe > Richtlinienoptionen > Schlüsseleinrichtung: Standard** in der Administrator-Oberfläche des PGP Universal Servers).

Für PGP Desktop-Benutzer ist der Client Key Mode aus folgenden Gründen die bessere Wahl:

- Viele PGP Desktop-Funktionen erfordern, dass die Benutzer ihre privaten Schlüssel verwalten. Wenn diese Schlüssel vom PGP Universal Server verwaltet werden, sind die entsprechenden Funktionen für die PGP Desktop-Benutzer nicht zugänglich.
- Im Server Key Mode sind bestimmte Optionen nicht verfügbar, die Sie für die PGP Desktop-Benutzer vorkonfigurieren. Beispielsweise ist die automatische Erstellung von PGP Virtual Disk-Laufwerken nicht möglich.

Manuelle Bindung an einen PGP Universal Server

Bei der manuellen Bindung an einen PGP Universal Server mit PGP Desktop (klicken Sie beim Anzeigen eines Messaging-Dienstes auf **Servereinstellungen**) und der Anmeldung laden Sie nur die E-Mail-Richtlinie und keine Consumer-Richtlinie herunter. Der PGP Universal Server-Administrator hat möglicherweise andere Optionen in der Consumer-Richtlinie festgelegt (z. B. Schlüsselmodi, Erzwingen der Verschlüsselung von Laufwerken usw.). Zur vollständigen Verwaltung und zum Erzwingen der Consumer-Richtlinie müssen Sie eine „gekennzeichnete“ Installation von PGP Universal Server verwenden. Wenden Sie sich an den Administrator, um bei Bedarf eine gekennzeichnete Installation zu erhalten.

Darüber hinaus ist bei der manuellen Bindung an einen PGP Universal Server die Datei `PGPtrustedcerts.asc` nicht unter C:\Dokumente und Einstellungen\Alle Benutzer\Anwendungsdaten\PGPCorporation\PGP vorhanden. Wenn Sie eine manuelle Bindung an einen PGP Universal Server durchführen möchten, müssen Sie diese Datei erstellen und sicherstellen, dass die Benutzer-ID des Organisationsschlüssels in dieser Datei dem durch PGPSTAMP angegebenen Server entspricht (Domänenname und IP-Adresse müssen übereinstimmen).

D PGP Desktop mit IBM Lotus Notes verwenden

In diesem Abschnitt wird die Verwendung von PGP Desktop mit Lotus Notes (einschließlich MAPI) beschrieben.

In diesem Kapitel

Informationen zur Kompatibilität von Lotus Notes und MAPI 361
PGP Desktop mit Lotus Notes verwenden 362
Bindung an einen PGP Universal Server 363
Notes-Adressen 365
Einstellungen des Notes-Clients 365
Native Verschlüsselung von Lotus Notes verwenden 366

Informationen zur Kompatibilität von Lotus Notes und MAPI

Nach der ordnungsgemäßen Konfiguration funktioniert PGP Desktop Messaging mit Lotus Notes- und MAPI-E-Mail-Clients in einer mit PGP Universal geschützten Umgebung auf dieselbe Weise wie mit POP- oder IMAP-E-Mail-Clients. Weitere Informationen hierzu finden Sie unter *E-Mail-Nachrichten sichern* (auf Seite 95). Die Informationen im vorliegenden Anhang ergänzen die Informationen in diesem Kapitel.

Lotus Notes ist eine Groupware-Anwendung, die Funktionen für Messaging sowie Kalender- und Planungsfunktionen bereitstellt. Informationen zu kompatiblen Lotus Notes-E-Mail-Clients finden Sie in den *Versionshinweisen zu PGP Desktop für Windows*.

MAPI (Messaging Application Programming Interface) ist eine Messaging-Architektur und eine Client-Schnittstelle, die in Microsoft Exchange-Umgebungen verwendet wird.

Die Kompatibilität von Lotus Notes und MAPI in PGP Desktop bedeutet, dass Sie unter Verwendung Ihres vorhandenen E-Mail-Clients Nachrichten mit der PGP-Technologie schützen und darüber hinaus auch die anderen Funktionen von Lotus Notes und MAPI nutzen können.

Die Installation von PGP Desktop ist sowohl mit der Lotus Notes-Installation für einzelne als auch für mehrere Benutzer kompatibel.

PGP Desktop mit Lotus Notes verwenden

Dieser Abschnitt bietet eine Übersicht über die Interoperabilität von PGP Desktop und PGP Universal in einer Lotus Notes-Umgebung.

E-Mail-Nachrichten an Empfänger in einer Lotus Notes-Organisation senden

Innerhalb der Lotus Notes-Umgebung unterstützt PGP Desktop die Verwendung der SMTP- wie auch der Notes-Adressierung.

Notes-Adressen verwenden

Lotus Notes-Clients, die PGP Desktop verwenden, können Notes-Adressen für die Schlüsselsuche nutzen. Wenn ein Lotus Notes-E-Mail-Client eine E-Mail-Nachricht sendet, erkennt der PGP Desktop-Client dies und fügt die Notes-Adresse automatisch dem Schlüssel hinzu. Dieser Schlüssel wird dann mit PGP Universal synchronisiert, um die Schlüsselsuche nach Notes-Adresse zu erleichtern.

Allen PGP Universal Server-Schlüsseln ist eine SMTP-E-Mail-Adresse zugeordnet (z. B. josem@beispiel.com). Die Schlüssel der Benutzer interner Lotus Notes-E-Mail-Clients weisen im Schlüssel zusätzlich zur SMTP-E-Mail-Adresse die Notes-Adresse auf, z. B. CN=josem/O=notes6@notes6. (Die Schlüssel externer Benutzer umfassen niemals eine Notes-Adresse, da der Kontakt mit externen Benutzern immer mithilfe ihrer SMTP-E-Mail-Adresse erfolgt.) Die Schlüssel interner Benutzer des Lotus Notes-E-Mail-Clients verfügen über beide Adressen, d. h. die SMTP-E-Mail-Adresse und die Notes-Adresse, da die Schlüsselanfrage von PGP Universal Satellite für Windows eine der beiden Adressen anführen könnte.

SMTP-Adressen für Empfänger mit PGP Desktop verwenden

Lotus Notes-Clients, die PGP Desktop verwenden, können SMTP-IDs für die Schlüsselsuche innerhalb der Organisation nutzen. Einige Lotus Notes-Unternehmen nutzen SMTP-IDs für die gesamte interne Kommunikation, während andere Unternehmen ihren Mitarbeitern die Wahl lassen. PGP Desktop ist mit beiden Konfigurationen kompatibel. In diesem Fall erstellt Lotus Notes die E-Mail-Nachricht in der Regel in MIME und der Proxy von PGP Desktop führt S/MIME aus.

E-Mail-Nachrichten an Empfänger außerhalb einer Lotus Notes-Organisation senden

Lotus Notes-Clients, die PGP Desktop verwenden, nutzen SMTP-IDs für die E-Mail-Weiterleitung und die Schlüsselsuche außerhalb der Organisation. PGP Desktop ist mit beiden Konfigurationen kompatibel. In diesem Falls erstellt Lotus Notes die E-Mail-Nachricht in MIME und der Proxy von PGP Desktop führt S/MIME oder PGP/MIME aus. Der Empfänger erhält und entschlüsselt die E-Mail-Nachricht.

Bindung an einen PGP Universal Server

Wenn Lotus Notes- oder MAPI-E-Mail-Clients mit PGP Desktop *in einer von PGP Universal geschützten Umgebung* verwendet werden, ist möglicherweise ein zusätzlicher Schritt bei der Einrichtung erforderlich, da sowohl Lotus Notes- als auch MAPI-E-Mail-Clients eine direkte Verbindung mit ihren Domino- bzw. Exchange-E-Mail-Servern herstellen müssen.

Die Informationen in diesem Abschnitt betreffen Sie nicht, wenn Sie PGP Desktop als eigenständige Anwendung verwenden, d. h. außerhalb einer von einem PGP Universal Server verwalteten Umgebung.

Sie müssen nicht nur mit den E-Mail-Servern kommunizieren, sondern auch eine Verbindung zum PGP Universal Server haben. Beide Anforderungen werden erfüllt, wenn eine Richtlinie für den jeweiligen E-Mail-Server vorhanden ist und eine zweite Richtlinie, die sowohl den E-Mail-Server als auch den PGP Universal Server einschließt.

Dies wird als Bindung bezeichnet und ermöglicht, dass der E-Mail-Client auf seinen E-Mail-Server zugreifen kann, um E-Mail-Nachrichten zu senden und zu empfangen, und auf seinen PGP Universal Server, um Schlüssel und Richtlinien abzurufen. Die Bindung wird, wie bereits erwähnt, mithilfe der Messaging-Richtlinien von PGP Desktop erreicht.

Es gibt zwei Möglichkeiten, die erforderlichen Messaging-Richtlinien von PGP Desktop zum Unterstützen der Bindung zu erstellen: Vorbindung und manuelle Bindung.

Vorbindung

Mittels Vorbindung konfiguriert der PGP-Administrator das Installationsprogramm von PGP Desktop mit den Informationen, die zum Erstellen der Bindung in den Messaging-Richtlinien von PGP Desktop erforderlich sind. Die Vorbindung bewirkt also, dass die richtigen Richtlinien bereits in PGP Desktop konfiguriert sind.

Manuelle Bindung

Bei der manuellen Bindung konfiguriert der PGP-Administrator das Installationsprogramm von PGP Desktop nicht mit den Informationen, die zum Erstellen der Bindung in den Messaging-Richtlinien von PGP Desktop erforderlich sind. Sie müssen diese Richtlinien selbst erstellen.

Damit Sie einen E-Mail-Server und einen PGP Universal Server manuell binden können, müssen Sie zuerst einen Dienst für den PGP Universal Server erstellen und dann einen anderen Dienst für den E-Mail-Server, der einen Verweis auf den PGP Universal Server beinhaltet.

So binden Sie einen E-Mail-Server und einen PGP Universal Server manuell mithilfe von Messaging-Richtlinien von PGP Desktop

1. Öffnen Sie PGP Desktop.
2. Klicken Sie auf das Bedienfeld „PGP Messaging“.
3. Klicken Sie unter dem vorhandenen eigenständigen Dienst auf **Universal Server <keiner>** und wählen Sie **Neu erstellen** aus.
4. Geben Sie im Menü „Neuer PGP Universal-Dienst“ den Namen des Universal Servers ein und klicken Sie auf **OK**.
5. Senden Sie sich unter Verwendung Ihres E-Mail-Clients selbst eine Nachricht. Für MAPI-Benutzer ist dies u. U. nicht erforderlich. Fahren Sie in diesem Fall mit Schritt 8 fort.
6. Klicken Sie im Dialogfeld **Vorgang auf Ihre Anforderung angehalten** auf **OK**.
7. Lesen Sie im Posteingang die E-Mail-Nachricht von „PGP Universal“. Das Dialogfeld „Assistent für die Erstellung eines PGP-Schlüssels“ wird angezeigt.
8. Klicken Sie auf **Weiter**.
9. Wählen Sie unter **Schlüsselverwaltung auswählen** im Bereich **Schlüsselmodus** eine Option aus und klicken Sie auf **Weiter**.
10. Wählen Sie im Bildschirm **Schlüsselquelle auswählen** die Option **PGP Desktop-Schlüssel** aus, wenn Sie PGP Desktop als eigenständige Anwendung verwenden. Wählen Sie andernfalls die Option **Neuer Schlüssel** oder **Schlüssel importieren** aus.
11. Klicken Sie auf **Weiter**.
12. Wählen Sie den Schlüsselsatz aus und klicken Sie auf **Weiter**.
13. Klicken Sie auf **Fertig stellen**.

Notes-Adressen

PGP Desktop-Schlüsseln ist in der Regel mindestens eine SMTP-E-Mail-Adresse zugeordnet, z. B. josem@beispiel.com.

PGP Desktop-Schlüssel von Benutzern eines Lotus Notes-E-Mail-Clients in einer von einem PGP Universal Server verwalteten Umgebung enthalten zusätzlich zu einer SMTP-E-Mail-Adresse auch ihre Notes-Adresse, z. B. `CN=josem/O=notes6@notes6`. (Die Schlüssel von Benutzern eigenständiger Versionen von PGP Desktop verfügen nicht über eine Notes-ID, sondern verwenden immer ihre SMTP-E-Mail-Adressen.)

Wenn Sie PGP Desktop und einen Lotus Notes-E-Mail-Client in einer von einem PGP Universal Server verwalteten Umgebung einsetzen und weitere Informationen erhalten möchten, wenden Sie sich an den PGP-Administrator.

Einstellungen des Notes-Clients

Wenn Sie PGP Desktop mit einem Lotus Notes-E-Mail-Client verwenden, müssen Sie sicherstellen, dass auf der Registerkarte „Server“ im Feld für die Home/Mail-Server-Einstellung des Standortdatensatzes des E-Mail-Clients der vollständige Notes-Name angegeben ist (host/orgName) und nicht nur der WINS-Host.

Die PGP Corporation empfiehlt, dass Sie auf der Registerkarte für grundlegende Einstellungen für das aktuelle Speicherort-Dokument eine Eingabe im Feld für die Internet-E-Mail-Adresse **vornehmen. OCNOTES verwendet dieses Feld zur Bestimmung der SMTP-E-Mail-Adresse des Benutzers. Fehlt dieses Feld, erstellt PGP Desktop anhand des Global Domain-Dokuments des Domino-Servers eine SMTP-E-Mail-Adresse für diesen Benutzer.**

Wenn Sie sich im „Inselmodus“ befinden und PGP Desktop nicht in der Lage ist, die Schlüssel bestimmter oder aller Empfänger zu finden, versucht PGP Desktop, die Nachricht erneut zu verschlüsseln, indem die Anwendung nach Schlüsseln sucht, wenn der Replikator die Nachricht an Ihren Homeserver sendet.

Wenn PGP Desktop den Schlüssel für einen Empfänger nicht findet und die native Verschlüsselungsoption von Notes aktiviert ist, ermöglicht PGP Desktop die Verschlüsselung der Nachricht durch Lotus Notes an die Empfänger, die von der PGP-Anwendung nicht verschlüsselt werden konnten.

Konfigurationsdatei „Notes.ini“

PGP Desktop aktualisiert die Konfigurationsdatei `notes.ini` und fügt folgenden Eintrag hinzu:

```
EXTMGR_ADDINS=nPGPNote.dll
```

Dieser Eintrag darf nicht geändert oder entfernt werden. PGP Desktop durchsucht die Datei `notes.ini` bei jedem Start. Wenn dieser Eintrag fehlt, wird er von PGP Desktop erneut eingefügt.

Native Verschlüsselung von Lotus Notes verwenden

Mit der nativen Verschlüsselung von Lotus Notes können Notes-Benutzer interne E-Mail-Nachrichten senden, die an den Notes-Schlüssel des Benutzers verschlüsselt sind. Wenn PGP Desktop für die Verwendung der nativen Verschlüsselung von Notes konfiguriert ist, können vertrauliche Informationen verschlüsselt an interne Benutzer gesendet werden, wenn beim Verfassen der Nachricht ein Kontrollkästchen aktiviert wird. Alle Lotus Notes-Benutzer verfügen über einen Notes-Schlüssel.

Wenn die E-Mail-Adresse im Feld „An“ dem Lotus Notes-Format (CN=Alice Cameron/O=Beispielunternehmen) entspricht und die native Verschlüsselung von Notes aktiviert ist, ermöglicht PGP Desktop, dass die E-Mail-Nachricht mit Lotus Notes verschlüsselt gesendet wird. Wenn die E-Mail-Adresse im Feld „An“ eine SMTP-Adresse ist (acameron@beispiel.com), verschlüsselt PGP Desktop die E-Mail-Nachricht an Ihren PGP-Schlüssel.

Die native Verschlüsselung von Notes ist sowohl für von PGP Universal Server verwaltete als auch für eigenständige Umgebungen verfügbar. Informationen zum Aktivieren der nativen Verschlüsselung von Notes in einer eigenständigen Umgebung finden Sie in *PGP-Wissensdatenbankartikel 1613* (https://support.pgp.com/?faq=1613).

PGP Desktop wendet die Messaging-Richtlinien für die Signier- und Verschlüsselungsschaltflächen auf alle ausgehenden Lotus Notes-Nachrichten an, wenn die Optionen zum Signieren und/oder Verschlüsseln ausgewählt wurden. Informationen zu diesen Richtlinien finden Sie unter *Informationen und Beispiele zu Sicherheitsrichtlinien* (auf Seite 122). Sind die Richtlinien in Ihrer eigenständigen Umgebung nicht vorhanden, müssen Sie sie erstellen.

So verwenden Sie die native Verschlüsselung von Notes

1. Verfassen Sie die Nachricht in Lotus Notes.
2. Aktivieren Sie in der Nachrichten-Symbolleiste die Optionen **Signieren** und/oder **Verschlüsseln** (sofern diese in der Vorlage verfügbar sind). Sind sie nicht verfügbar, wählen Sie im Bereich für Sicherheitsoptionen die Option für Lieferoptionen aus. Aktivieren Sie die Optionen **Signieren** und/oder **Verschlüsseln**.

   Hinweis: Diese Optionen müssen jedes Mal aktiviert werden, wenn Sie eine E-Mail-Nachricht unter Verwendung der nativen Verschlüsselung von Notes senden möchten.

3. Senden Sie die Nachricht.

- Wenn die E-Mail-Richtlinie für die Verschlüsselung eingerichtet und der E-Mail-Empfänger ein Notes-Benutzer ist, wird die Nachricht unter Verwendung der nativen Verschlüsselung von Notes verschlüsselt gesendet. Klicken Sie in der Notifer-Meldung auf **Mehr**, um zu überprüfen, ob die Nachricht mit Lotus Notes verarbeitet und verschlüsselt wurde. Wenn der Empfänger die Nachricht öffnet, ist keine PGP-Anmerkung enthalten.
- Wenn die E-Mail-Richtlinie für die Verschlüsselung eingerichtet und der E-Mail-Empfänger eine SMTP-Adresse ist, sucht PGP Desktop den PGP-Schlüssel und die Nachricht wird mit PGP Desktop verschlüsselt gesendet. Wenn der Empfänger die Nachricht öffnet, ist die standardmäßige PGP-Anmerkung enthalten.
- Wenn die E-Mail-Richtlinie für die Verschlüsselung eingerichtet, der E-Mail-Empfänger eine SMTP-Adresse ist und Sie mit dem Lotus Notes Domino-Server verbunden sind, versucht Lotus Notes, die SMTP-Adresse auf die Lotus Notes-Adresse aufzulösen. Ist dies erfolgreich, wird die Nachricht unter Verwendung der nativen Verschlüsselung von Notes gesendet. Klicken Sie in der Notifer-Meldung auf **Mehr**, um zu überprüfen, ob die Nachricht mit Lotus Notes verarbeitet und verschlüsselt wurde. Wenn der Empfänger die Nachricht öffnet, ist keine PGP-Anmerkung enthalten.
- Wenn die E-Mail-Richtlinie für das Signieren eingerichtet ist, signiert Lotus Notes die Nachricht mit dem Notes-Schlüssel des Absenders. Es erfolgt keine Verschlüsselung mit Lotus Notes oder PGP Desktop. Wenn die Option zum **Signieren der Nachricht nicht aktiviert ist, signiert PGP Desktop die Nachricht mit dem PGP-Schlüssel des Absenders.**

Index

A

Active Directory-Gruppen in PGP NetShare - 273, 274
Adressenlisten-Richtlinien - 122, 123, 124, 125, 128
AES, Algorithmus in PGP Virtual Disk - 237
akustische Signale, PGP WDE-Authentifizierung - 187
akustische Signale, während PGP WDE-Authentifizierung - 187
Aladdin eToken Pro USB Token - 168, 172, 175, 323
allgemeine Optionen - 327
anmelden im PGP Bootguard-Bildschirm - 184
Anwendernamen, auf Schlüsseln - 64
Anwendungen, Erzwingen oder Umgehen der Verschlüsselung von - 256
Anwendungsfenster - 30
Archive - 287
  bearbeiten - 301
  erstellen - 288
  erweiterte Optionen - 288
  Nur signieren - 298
  öffnen - 299, 301
  selbstentschlüsselnd - 296, 300
  verifizieren, signierter - 303
ausgehende E-Mail-Nachrichten - 98
ausgesperrt, im PGP BootGuard-Bildschirm - 188
Authentifizierung für PGP Whole Disk Encryption - 167, 187, 195
  akustische Signale während - 187
  Umgehen in PGP WDE - 195
  verwendete Methode, festlegen - 167
Authentifizierung über das Trusted Platform Module (TPL) - 169
automatische Aktivierung von PGP Virtual Disk-Datenträgern - 221
automatische Sicherungssoftware, auf PGP WDE-verschlüsselten Laufwerken verwenden - 202

B

BartPE, mit PGP WDE verwenden - 215
Bedienfeld - 30
Benutzer - 230, 268
  geschützte Ordner, aktiviert in - 250, 268, 269, 272
  PGP NetShare, Zugriffslisten importieren in - 272
  PGP Whole Disk Encryption, hinzufügen oder löschen aus - 196, 197
Benutzeroberfläche, Hauptfenster - 30
berechtigte Benutzer, in PGP NetShare - 250, 268
Bewertungslizenzen - 7
biometrische Wortliste, Erläuterung - 62
BootGuard - See PGP BootGuard-Bildschirm
bypass, PGP WDE SSO login - 193

C

CACs - 312
CAST, Algorithmus in PGP Virtual Disk - 237
Client-Schlüsselmodus (CKM) - 136
Common Access Cards (CACs) - 312
CPU-Auslastung, während Verschlüsselung - 175

D

Dateien
  Dateien, dauerhaft löschen - 307
  Eigenschaften von, PGP NetShare - 280
  negativ gelistet in PGP NetShare - 255
  öffentliche Schlüssel exportieren - 53
  schützen außerhalb eines geschützten Ordners - 277
  verwenden in geschützten Ordnern - 263, 264, 265
Dateien sicher löschen - See Dateien vernichten, See sicheres Löschen von freiem Speicherplatz
Dateien vernichten - 305
Dateien, dauerhaft löschen - 307
Daten von einem verschlüsselten Laufwerk wiederherstellen - 209
Datenwiederherstellung - 209
Dauerlizenzen - 7
deinstallieren - 26, 202
designierter Widerrufer - 83
Dialogfeld Windows-Anmeldung, anzeigen - 193

Dienste - 103
Dienste, Messaging - 103, 104, 106, 111
digitale Signaturen - 51, 54, 69, 77, 94, 291, 293, 298
Dritthersteller-Software, Kompatibilität mit - 166, 202

E

Eigenschaften - 62, 282, 315
eingehende E-Mail-Nachrichten - 97
Einrichtungsassistent - 26
Einzelanmeldung - 167, 190
  anmelden bei PGP WDE - 192
  mit PGP WDE verwenden - 190, 191, 192
  Passphrase, ändern - 192, 198
  Umgehen, in PGP WDE - 193
Einzelplatzanwender - 5
E-Mail - 95
  Dienste und Richtlinien - 103
  mehrere Konten - 111
  Messaging-Protokoll - 140
  Notifier - 36
  öffentliche Schlüssel kopieren aus - 56
  öffentlichen Schlüssel anhängen - 53
  Optionen - 337
  Schlüsselmodi - 136
  schützen - 95
Energiesparmodus, Mac OS X und PGP WDE - 215
entfernen - 63, 81, 320
Entschlüsseln - 212
erstellen - 44, 106, 114, 221, 288, 353
  Messaging-Dienst - 106
  Messaging-Richtlinie - 114
  Passphrasen, starke - 353
  PGP Virtual Disk-Datenträger - 221
  PGP Zip-Archiv - 288
  Schlüsselpaar - 44, 316
exportieren
  Schlüssel in Datei - 53
  Schlüssel von einer Smartcard - 318

F

Fehlerbehebung - 10, 112, 183
Fingerabdruck, digitalen verifizieren - 71
FIPS - 347
Forensik, Datenwiederherstellung - 209
Foto-ID auf Schlüsseln - 63
Freien Speicherplatz sicher löschen - See sicheres Löschen von freiem Speicherplatz

G

geschützte Ordner - 258, 282, See geschützte Ordner
  Active Directory-Gruppen - 273
  Benutzer, in geschützten Ordnern - 253, 254, 268, 272, 273
  Dateien anzeigen in - 265
  Dateien, verwenden außerhalb von - 277
  Dateien, verwenden in - 263, 265
  Eigenschaften - 282
  entfernen - 275
  entsperren - 264
  erstellen - 260
  Lizenzierung - 253
  negativ gelistete Dateien in - 255
  Sichern von Dateien und Ordnern - 279
  Speicherort, festlegen - 258
  Status von - 266
  umschlüsseln - 276
  Unterordner in - 266
  Zugriffslisten, importieren - 272
geschützte Ordner entsperren - 264
geteilte Schlüssel wieder zusammenfügen - 85, 87
Grundbegriffe - 5, 13, 17, 103, 136, 250
Grundlegende Schritte für die Verwendung - 18
Guarded Key Mode (GKM) - 136

H

Hauptschlüsseloptionen - 58, 59, 333

I

IBM Lenovo Rescue & Recovery - 216
Ihre Passphrase ändern - 68
importieren, private Schlüssel und Zertifikate - 65
IM-Sitzungen verschlüsseln - 95, 143, 149, See PGP Messaging
Informationen zu schreibgeschützten Laufwerken oder Partitionen - 194
Instant Messaging - 143

Optionen - 338
Sitzungen verschlüsseln - 145

J

JavaCards - 312

K

Kennwörter - See Passphrasen
Keyserver - 15, 56
durchsuchen - 55
fremde öffentliche Schlüssel abrufen - 55
Liste von - 330
öffentlichen Schlüssel senden an - 51
zur Verteilung widerrufener Schlüssel verwenden - 84
Keyserver durchsuchen - 55
komprimieren, PGP Virtual Disk-Laufwerk - 228
Kontextmenüs, in PGP Netshare - 280
Koordinator für PGP NetShare - 254
Kryptographie - 18

L

Laufwerke
Anwender zu verschlüsselten Laufwerken hinzufügen - 196
entfernbar - 203, 205
Fehler während Verschlüsselung - 183
geplantes sicheres Löschen - 309
Optionen - 342
unterstützt in PGP WDE - 160
verschlüsseln - 177, 179
Verwendung, verschlüsselt - 184
Wiederherstellung, erstellen - 210
Laufwerk-Notifier - 39
Lese-/Schreibfehler - 179
Lizenzierung - 7, 8, 26, 158, 253
lokale Anwender - 191, 199
lokale Richtlinie - See Offline-Richtlinie
löschen
Benutzer - 231, 272
Benutzer-IDs - 69
Dateien, dauerhaft löschen - 307
Messaging-Richtlinie - 133
PGP Virtual Disk-Laufwerke - 234
Schlüssel - 69, 320
Signatur aus öffentlichem Schlüssel - 74
Unterschlüssel - 81
Lotus Notes E-Mail-Client - 361, 365, 366

M

Mail-Server, siehe Messaging-Dienste - See Messaging
MAPI - 361
mehrere Messaging-Services - 111
Messaging - 103
bestehende bearbeiten - 110
deaktivieren und aktivieren - 110
Fehlerbehebung - 112
löschen - 110
Lotus Notes - 361
MAPI - 361
mehrere - 111
Messaging-Protokoll - 140
Neu erstellen - 106
Notifier - 36
Optionen - 334
Mietlizenzen - 7

N

negativ gelistet, in PGP NetShare - 255, 256
NetShare - See PGP NetShare
Notes-ID - See Lotus Notes E-Mail-Client
Notifier - 36, 345
Notifier-Funktion
Beschreibung - 36
für Instant Messaging - 39
Notifier-Meldungen für ausgehende E-Mail-Nachrichten - 37
Notifier-Meldungen für eingehende E-Mail-Nachrichten - 37

O

öffentliche Schlüssel - 15

an andere Personen verteilen - 51
an Keyserver senden - 51
andere öffentliche Schlüssel abrufen - 54
aus E-Mail-Nachrichten kopieren - 56
authentifizieren mit in PGP WDE - 168
deaktivieren und aktivieren - 70
E-Mail-Nachricht, anhängen an - 53
in Datei exportieren - 53
in Datei speichern - 53
Keyserver durchsuchen - 55
kopieren von einer Smartcard - 318
PGP Whole Disk Encryption - 168
signieren - 72
verifizieren - 71
Vorteile des Versands an einen Keyserver - 51
Offline-Richtlinie - 38, 98, 101, 104
Optionen - 325
allgemein - 327
Erweitert - 347
Hauptschlüssel - 333
Instant Messaging - 334, 338
Laufwerk - 342
Messaging - 334
Notifier - 340
PGP NetShare - 277, 340
Proxy - 336
Schlüssel - 330
Verschlüsselung - 170, 175
Ordner sicher löschen - 307, 309
Ordner, geschützt in PGP NetShare - 250

P

Partitionen, verschlüsseln - 160, 171, 177, 195
Passphrase
vergessen - 355
Passphrasen - 47, 238, 351
alternativ, hinzufügen - 196, 230
Alternative für PGP Virtual Disk hinzufügen - 196
ändern - 68, 192, 197, 233, 246, 319
authentifizieren mit in PGP WDE - 167
Einzelanmeldung - 167
festlegen - 44
Löschen zwischengespeichert - 277
Optionen - 327
PGP Whole Disk Encryption - 167
stark, erstellen - 353
unterstützte Zeichen in PGP WDE - 178
vergessen - 89
verschlüsseln mit in PGP Zip - 293
Passphrasen-Qualitätsanzeige - 352
Passphrase-Qualitätsanzeige - 352
PGP BootGuard-Bildschirm - 178, 184, 187, 188
PGP Desktop
Beschreibung - 13
deinstallieren - 26
Einrichtungsassistent - 26
Hauptbildschirm - 29, 30
in einer von PGP Universal verwalteten Umgebung - 358
installieren - 23
PGP-Symbol in der Taskleiste - 31
Richtlinienbeschreibung - 103
SSL/TLS-Support - 134
Systemvoraussetzungen - 21
Upgrade durchführen - 23
PGP Desktop auf einen anderen Computer übertragen - 27
PGP Desktop installieren - 21
PGP Desktop-Protokoll - 41
PGP Global Directory - 13, 56
PGP Keys - See Schlüssel
Schlüsselpaar erstellen - 44
PGP Messaging - 13, 95, 140
Dienste und Richtlinien - 103
Dienstebeschreibung - 103
PGP NetShare - 13, 249, See geschützte Ordner

Active Directory-Gruppen - 273, 274
anwendungsbasierte Verschlüsselungsliste - 256
Bearbeitungsmenüoptionen - 283
Benutzer - 268, 272, 273
beschädigte, gelöschte oder überschriebene Dateien, Verwendung von - 260
Dateimenüoptionen - 283
Eigenschaften von Datei oder Ordner - 280
Koordinator definieren - 254
Lizenzierung - 253
negativ gelistete Dateien - 255, 256
Netshare-Menüoptionen - 284
Notifier - 39
Optionen - 277
Ordnerstatus überprüfen - 266
Passphrase löschen - 277
PGP Virtual Disk oder PGP WDE, verwenden mit - 250
positiv gelistete Ordner - 256
Rollen - 252, 270
Sichern von geschützten Dateien - 279
Umgehungsanwendungen für die Entschlüsselung - 256
Von PGP Universal verwaltete Umgebung - 281
Zugriffslisten aus einem anderen Ordner importieren - 272
PGP Shredder - 13, 305
Dateien, dauerhaft löschen - 307
PGP Zip, verwenden mit - 288
sicheres Löschen von freiem Speicherplatz - 308, 309
PGP Universal - 89, 357
PGP Universal Server - 6, 13, 44, 56, 89, 90, 206, 281, 347, 357, 359, 362
PGP Universal-Dienstprotokoll (USP) - 56
PGP Virtual Disk - 13, 219, 237
aktivieren - 221, 226
alternative Benutzer - 230
Austauschen - 236
deaktivieren - 226, 227
Finden - 225
Neu erstellen - 221
Passphrasen, ändern - 233
pflegen - 235
Sicherheitsmaßnahmen - 237
Sichern - 235
umschlüsseln - 228
Verschlüsselungsalgorithmen - 237
PGP Virtual Disk-Datenträger - 226, 227
PGP Virtual Disk-Laufwerke aktivieren - 226
PGP Whole Disk Encryption - 13, 155

Authentifizierung mit einem öffentlichen Schlüssel - 168
Authentifizierungsoptionen - 167, 195
automatische Sicherungssoftware - 202
Benutzern, arbeiten mit - 196, 197
deinstallieren - 202
Einzelanmeldung, verwenden mit - 167, 190, 192, 193
Kompatibilität mit Anwendungen von Drittherstellern - 166
Laufwerk verschlüsseln - 179
Laufwerk vorbereiten für - 159
Laufwerk, PGP WDE-verschlüsseltes verwenden - 184
Laufwerk, Schutz aufrechterhalten vom - 194
Laufwerksfehler während der Verschlüsselung - 179, 183
Laufwerkstypen, unterstützte - 160
Lizenzierung - 158
Notifier - 39
Optionen bei Laufwerkverschlüsselung - 165, 170, 175
Partitionen - 171
Passphrase - 167, 178, 192, 197, 200
PGP BootGuard-Bildschirm - 184, 187
PGP Universal Server, verwaltet - 206
Sicherheitsmaßnahmen - 213
Stromversorgung, während Verschlüsselung - 165
Tastaturbelegungen - 188
Token-basierte Authentifizierung - 168, 172
unterstützte Laufwerkstypen - 160
verschlüsseltes Laufwerk entschlüsseln - 212
verschlüsseltes Laufwerk umschlüsseln - 199
Verschlüsselungsdauer, berechnen - 164
Verschlüsselungsoptionen - 170, 175
verwendeter Verschlüsselungsalgorithmus - 161
Wechseldatenträger - 203, 205
Wiederherstellungsdatenträger erstellen - 210
Wiederherstellungs-Token - 208
PGP Zip - 13, 287
Änderungen speichern - 301
Archiv, erstellen - 288
Archive verschlüsseln - 291, 293
Dateien extrahieren aus - 301
Dateien nach Archivierung vernichten - 288
ein Archiv bearbeiten - 301
ein Archiv öffnen - 299, 301
eine Datei oder einen Ordner hinzufügen - 301
eine Datei oder einen Ordner löschen - 301
erweiterte Optionen, Archiv erstellen - 288
Nur signieren - 298
selbstentschlüsselnde Archive - 296, 300
signierte Archive verifizieren - 303
PGP-Administrator - 206, 357, 358
PGP-Keyserver-Liste - See Keyserver
PGP-Protokoll - 41
PGP-Symbol in der Taskleiste - 31
PKCS-11-Bibliothek - 312
PKCS-12-X.509-Zertifikate, importieren - 65
Platzhalter, in Richtlinien - 120
positiv gelistet, in PGP NetShare - 256
primärer Name auf dem Schlüssel - 64, 65
private Schlüssel - 15, 44, 48, 65
Protokoll, Messaging - 41, 140

R

Rescue & Recovery - See IBM Lenovo Rescue & Recovery
Richtlinie aktualisieren - 31, 101
Richtlinien - 103
Beispiele für Messaging - 122
löschen - 133
Messaging erstellen - 114
Reihenfolge ändern - 134
Standardrichtlinien - See Standardrichtlinien
Rollen, in PGP NetShare - 252, 270
Ruhezustand - 214, 238, See Energiesparmodus, Mac OS X und PGP WDE

S

Schlüssel - 43, 61

aktivieren - 70
anzeigen - 43
aus dem Schlüsselbund löschen - 69
deaktivieren - 70
Eigenschaften - 62
E-Mail, anhängen an - 53
erstellen - 44
exportieren - 53, 318
Foto-ID ersetzen - 63
geteilten Schlüssel wieder zusammenfügen - 85, 87
Hauptschlüssel - 58
importieren - 65
Keyserver, hochladen auf - 53
mehrere Anwendernamen und E-Mail-Adressen - 64
öffentliche Schlüssel in Datei speichern - 53
öffentliche Schlüssel verifizieren - 71
Optionen - 330
schützen - 94
signieren - 72, 74
teilen - 85
Unterschlüssel - 75
verloren - 89
vertelen, öffentlicher - 51
Vertrauen für Validierungen gewähren - 74
widerrufen - 83, 84
wiederherstellen - 89
Schlüssel oder Passphrase verloren - 89
Schlüssel schützen - 94
Schlüssel teilen - 85
Schlüssel und Signaturen widerrufen - 74, 81, 84
Schlüssel validieren - 74
Schlüssel wiederherstellen - 50, 89, 200
Schlüsselbunde - 43, 49, 69
Schlüssel-ID - 62
Schlüsselmodi - 136, 347
Schlüsselmodus zurücksetzen - 136, 347
Schlüsselpaar - 15
erstellen - 44
Smartcard - 316, 319
Schlüsselpaare erstellen - 44, 316
Schlüssel-Wiederherstellung - 89, See Schlüssel wiederherstellen
selbstentschlüsselnde Archive - 296, 300
separater Signatur-Unterschlüssel - 13
Server Client Key Mode (SCKM) - 136
Server-Schlüsselmodus (Server Key Mode, SKM) - 136
sicher löschen, Schlüssel von Smartcard - 320
Sichere Instant Messaging-Anwendung (IM) - 143
sicheres Löschen des freien Speicherplatzes planen - 309
sicheres Löschen von freiem Speicherplatz - 13, 307, 308, 309
Sicherheitsmaßnahmen - 213, 237
Sichern von Schlüsseln - 50
Sicherungssoftware, verwenden - 202, 279
Signaturen, aus Schlüsseln löschen - 69, 74
signieren - 69
Archive in PGP Zip - 298, 301
öffentliche Schlüssel - 72
Schlüssel - 69, 72
signierte PGP Zip-Archive verifizieren - 303
Smartcard - 15, 311
authentifizieren mit, bei PGP BootGuard - 173
Eigenschaften - 315
Ihren öffentlichen Schlüssel kopieren aus - 318
JavaCards - 312
Karten, in PGP WDE unterstützt - 173
Leser, in PGP WDE unterstützt - 173
Passphrase ändern - 319
Personalisierung - 312
PKCS-11 - 312
Schlüssel sicher löschen von - 320
Schlüsselpaar kopieren in - 319
Schlüsselpaar, neu erstellen auf - 316
Sprachunterstützung für PGP WDE - 188
SSL/TLS-Support - 134
Standardrichtlinien - 103, 122, 123, 124, 125
Standby, PGP WDE - 214
starke Passphrasen - 353
Startmenü - 35
Stromausfallschutz (Option) - 175
Support, Kontaktaufnahme - 11, 12
Systemvoraussetzungen - 21, 160, 166, 172, 175

T

Tasks, geplantes Löschen von freiem Speicherplatz - 309
Tastatur, in PGP WDE unterstützt - 161, 188
Tastaturbefehle - 347

technischer Support - 12
technischer Support, Kontaktaufnahme - 11
Token - 172, 311
  authentifizieren mit in PGP WDE - 168
  Eigenschaften - 315
  ein neues Schlüsselpaar erstellen auf - 316
  kopieren in oder aus - 318, 319
  PGP Whole Disk Encryption, verwenden mit - 168, 172
  Schlüssel sicher löschen von - 320
  unterstützte Token in PGP WDE - 173
TPM - See Authentifizierung über das Trusted Platform Module (TPL)
Tray-Symbol - See PGP-Symbol in der Taskleiste
Twofish, Algorithmus in PGP Virtual Disk - 237

U

Übersicht, über PGP Desktop - 1
umschlüsseln - 199, 276
Universal Server - See PGP Universal
Unterschlüssel - 75
  Ablaufdatum - 75, 78
  ansehen - 78
  anzeigen - 75
  arbeiten mit - 75
  Eigenschaften - 75
  entfernen - 81
  Größe - 75
  Größe festlegen von - 78
  Gültigkeit - 75
  Neu erstellen - 78
  separat - 75
  signieren - 78
  Symbole - 75
  Verschlüsseln und Signieren - 78
  Verschlüsselung - 78
  widerrufen - 81
Unterschlüssel anzeigen - 75
Upgrade durchführen - 23, 25
USP - See PGP Universal-Dienstprotokoll (USP)

V

vergessene Passphrasen - 89
verschlüsselte Wechsellaufwerke neu formatieren - 205
Verschlüsselung
  Anwender aus PGP WDE löschen - 197
  Anwender hinzufügen - 196
  Dauer berechnen in PGP WDE - 164
  Empfängerschlüssel in PGP Zip - 291
  Instant Messaging-Sitzungen - 145
  Laufwerk oder Partition umschlüsseln - 199
  Laufwerke oder Partitionen - 177, 179
  Laufwerksfehler während - 179, 183
  Maximale CPU-Auslastung (Option) - 164, 175
  Optionen in PGP WDE - 170
  Partitionen in PGP WDE - 171
  Passphrase in PGP Zip - 293
  PGP WDE-verschlüsselte Laufwerke verwenden - 184, 206
  Pilottest - 166
  Reduzieren der Zeit für die Erstverschlüsselung - 164, 175
  Stromausfallschutz (Option) - 165, 175
  verwendeter Algorithmus - 161, 237
Vertrauen gewähren - 74
Vertrauen, für Schlüsselvalidierungen gewähren - 74
Virtual Disk-Laufwerke verteilen - 236
virtuelle Laufwerke - See PGP Virtual Disk
virtuelle Laufwerke austauschen - 236

W

Warnungen - See Notifier
Wechseldatenträger in PGP WDE - 203, 204, 205
Widerrufer, Schlüssel - 83
Wiederherstellungsdatenträger in PGP WDE erstellen - 210
Wiederherstellungs-Token - 208
Windows Explorer - 34
Windows-Vorinstallationsumgebung (PE), verwenden mit PGP WDE - 215
WINS-Host - 365
Wortliste, biometrische - 62

X

X.509-Zertifikate - 65

Z

Zeichen, in PGP WDE unterstützt - 178
zentral verwaltete Anwender - 5
Zugriffslisten importieren in PGP NetShare - 272

Zusätzliche Verschlüsselungsschlüssel
(Additional Decryption Keys, ADK) - 81